



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2009-12

Deterrence of nuclear terrorism via
post-detonation attribution is the United
States on target?

Geelhood, Philip.

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/4451>

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**DETERRENCE OF NUCLEAR TERRORISM VIA POST-
DETONATION ATTRIBUTION:
IS THE UNITED STATES ON TARGET?**

by

Philip Geelhood

December 2009

Thesis Advisor:
Second Reader:

Jeffrey Knopf
Zachary Davis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Deterrence of Nuclear Terrorism via Post-Detonation Attribution: Is the United States on Target?			5. FUNDING NUMBERS	
6. AUTHOR(S) Philip Geelhood				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) As nuclear terrorism is a risk of low probability and high consequences, the United States is right to address it as a significant—but not the utmost—national security priority. The science of nuclear forensics makes possible the characterization of nuclear materials used in a nuclear attack, and, as such, provides the backbone of an attribution program. Nuclear forensics-based attribution serves the dual purpose of helping to prevent nuclear terrorism by enabling deterrence, as well as guiding and enabling post-attack response options in the event of deterrence failure. The deterrence that an attribution capability alone enables is fairly narrow in its effective scope, though this deterrence does cover what would otherwise be a critical gap in U.S. strategy for preventing nuclear terrorism. The U.S. attribution capability is currently lacking in several important regards, the most significant of which is a future dearth of highly qualified personnel. Since an attribution capability is a critical enabler, the United States must do more to efficiently develop its attribution program. This can be done most cost-effectively in the short term by focusing on unilateral program needs while building an enduring domestic political will to improve and then maintain the nation's attribution capability.				
14. SUBJECT TERMS Nuclear Terrorism, Nuclear Forensics, Attribution, Deterrence, Risk of Nuclear Terrorism, Probability of Nuclear Terrorism, Consequences of Nuclear Terrorism, Post-detonation Response			15. NUMBER OF PAGES 111	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**DETERRENCE OF NUCLEAR TERRORISM VIA POST-DETONATION
ATTRIBUTION: IS THE UNITED STATES ON TARGET?**

Philip Geelhood
Major, United States Air Force
B.S., Cedarville University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2009**

Author: Philip Geelhood

Approved by: Dr. Jeffrey Knopf
Thesis Advisor

Dr. Zachary Davis
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As nuclear terrorism is a risk of low probability and high consequences, the United States is right to address it as a significant—but not the utmost—national security priority. The science of nuclear forensics makes possible the characterization of nuclear materials used in a nuclear attack, and, as such, provides the backbone of an attribution program. Nuclear forensics-based attribution serves the dual purpose of helping to prevent nuclear terrorism by enabling deterrence, as well as guiding and enabling post-attack response options in the event of deterrence failure. The deterrence that an attribution capability alone enables is fairly narrow in its effective scope, though this deterrence does cover what would otherwise be a critical gap in U.S. strategy for preventing nuclear terrorism. The U.S. attribution capability is currently lacking in several important regards, the most significant of which is a future dearth of highly qualified personnel. Since an attribution capability is a critical enabler, the United States must do more to efficiently develop its attribution program. This can be done most cost-effectively in the short term by focusing on unilateral program needs while building an enduring domestic political will to improve and then maintain the nation's attribution capability.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH FOCUS.....	1
B.	BACKGROUND	1
1.	Importance.....	1
2.	Problems and Hypothesis	3
3.	Program Origins and Current Organization	4
C.	LITERATURE REVIEW	5
D.	METHODOLOGY	6
E.	THESIS OVERVIEW	7
F.	FINDINGS	7
II.	ASSESSING THE THREAT OF NUCLEAR TERRORISM	9
A.	OVERALL ASSESSMENTS OF THE RISK	10
B.	RISK COMPONENTS	11
1.	Consequences.....	11
2.	Probability—Intent.....	12
3.	Probability—Capability	13
4.	Probability—Vulnerability	18
C.	CURRENT MITIGATION EFFORTS.....	20
D.	CHAPTER SUMMARY.....	25
III.	DETERRENCE THEORY	27
A.	WHO?	27
B.	PRECISELY WHAT ACTION?	28
C.	WHOM?.....	31
D.	HOW CONVINCING?.....	35
1.	Commitment—Clearly Defined and Communicated	36
2.	Capability.....	36
3.	Intent	38
E.	DETERRENCE FAILURE.....	41
F.	IMPLICATIONS AND POLICY RECOMMENDATIONS	43
G.	CHAPTER SUMMARY.....	45
IV.	POST-DETONATION ATTRIBUTION CAPABILITY	47
A.	NUCLEAR FORENSICS—SOME DEFINITIONS.....	48
B.	NUCLEAR FORENSICS IN THE CONTEXT OF ATTACK ATTRIBUTION—THE PROCESS	48
C.	OVERALL CURRENT CAPABILITY ASSESSMENT	53
D.	PROGRAM COMPONENTS.....	56
1.	Scientific Limitations and Requirements.....	56
2.	Nuclear Materials Database.....	57
3.	Intelligence Support.....	61
4.	Law Enforcement Support.....	63

5.	Exercise Requirements	66
E.	COSTS TO IMPROVE AND SUSTAIN	67
F.	CHAPTER SUMMARY	69
V.	CONCLUSION	71
A.	REVIEW OF KEY FINDINGS	71
1.	Importance of an Attribution Program	71
2.	Reliability and Accuracy Necessary for Effective Deterrence	72
3.	The Appropriate Deterrence Posture and Its Credibility	72
4.	Role of Nuclear Forensics and Overall State of Attribution Program	73
5.	Costs to Close the Gap	74
B.	OVERALL POLICY RECOMMENDATIONS	74
1.	Current Capability Maximization	75
2.	Investment for the Future	76
3.	Deterrence Posture	77
4.	For Further Research	78
C.	CONCLUDING THOUGHTS	80
	LIST OF REFERENCES	83
	BIBLIOGRAPHY	91
	INITIAL DISTRIBUTION LIST	97

LIST OF ACRONYMS AND ABBREVIATIONS

AFTAC	Air Force Technical Applications Center
CBP	Customs and Border Protection
C	Consequences
CIA	Central Intelligence Agency
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership against Terrorism
CTR	Cooperative Threat Reduction
DHS	Department of Homeland Security
DNEA	Domestic Nuclear Event Attribution
DoD	Department of Defense
DoE	Department of Energy
DoJ	Department of Justice
DoS	Department of State
DTRA	Defense Threat Reduction Agency
FBI	Federal Bureau of Investigation
GTRI	Global Threat Reduction Initiative
HEU	Highly-Enriched Uranium
HR	House Resolution
HUMINT	Human Intelligence
IAEA	International Atomic Energy Agency
IC	Intelligence Community
IED	Improvised Explosive Device
IND	Improvised Nuclear Device
MASINT	Measurement and Signature Intelligence
NTNF	National Technical Nuclear Forensics
NTNFC	National Technical Nuclear Forensics Center
P	Probability
PSI	Proliferation Security Initiative
R	Risk
RDD	Radiological Dispersal Device

SNM	Special Nuclear Material
T	Threat
TOPOFF	Top Officials
V	Vulnerability
WMD	Weapons of Mass Destruction

ACKNOWLEDGMENTS

“Praise be to the Lord, to God our Savior, who daily bears our burdens.”
(Psalms 68:19, NIV)

I would like to thank my family: my wife, Tara, who as my best friend provided tremendous support and encouragement always; and my three small children, whose almost daily questioning, (“Daddy, have you finished your papers yet?”), was often all the motivation I needed.

Additionally, I am indebted to my Thesis Advisor, Dr. Jeffrey Knopf, and Second Reader, Dr. Zachary Davis. Dr. Davis supplied the initial enthusiasm and direction needed to get me started on the right track. Dr. Knopf expertly and patiently guided me throughout the course of this project. Thank you both very much.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH FOCUS

In this thesis, I examine the role of post-detonation nuclear forensics in the effort to identify the source of nuclear materials used in a terrorist nuclear attack on the U.S. Homeland. The U.S. government desires such an attribution capability in order to deter the transfer of nuclear weapons or materials from states to terrorist actors, as well as to inform post-attack response options should deterrence fail.¹ I will assess whether a perfect attribution capability is required for effective deterrence, or if a less-than-perfect capability will suffice. In order to identify existing critical gaps, I will also consider the levels of reliability and accuracy with regard to forensic technology and intelligence support required for a sufficient attribution capability. If the United States does not currently possess these levels of reliability and accuracy, are they achievable in the near term and at a cost it can afford to pay? I will explore these questions against the backdrop of an open-source threat assessment and a review of relevant deterrence theory, with the ultimate goal of recommending the priority the United States should place on its pursuit of such an attribution capability.

B. BACKGROUND

1. Importance

The U.S. government has been concerned with the potential for clandestine nuclear attack since 1946, and nuclear terrorism in particular since the early 1970s.² The threat took on an entirely new dimension in the 1990s with the emergence of well-funded and religiously-motivated transnational terrorist organizations with a demonstrated intent to indiscriminately inflict casualties and destruction on a massive scale. Terrorist groups

¹ Office of the President of the United States of America, *National Strategy for Combating Terrorism* (Washington, DC: Government Printing Office, 2006), 14–15.

² Jeffrey T. Richelson, *Defusing Armageddon: Inside NEST, America's Secret Nuclear Bomb Squad* (New York, NY: W. W. Norton & Company, Inc., 2009), 1–14.

have pursued nuclear weapons in the past and are likely to continue to do so in the future.³ In light of this threat, the denial of a nuclear capability to terrorist groups is of critical importance.

States alone are realistically capable of manufacturing the fissile materials necessary for nuclear weapons; therefore, terrorists are left to beg, borrow, steal, or otherwise be entrusted by a state with fissile materials or an entire weapon itself.⁴ Graham Allison, in asserting that nuclear terrorism is preventable, encapsulates the problem and its ideal solution thusly: “No fissile material, no nuclear explosion, no nuclear terrorism. It is that simple.”⁵ Generally, states can become a source of nuclear fissile materials or nuclear weapons for terrorists in two ways—either through intentional transfer or through negligent disregard for the security of state nuclear assets. The U.S. government has pursued policies and programs intended to address every aspect of this problem.

The strategies designed to prevent terrorists from acquiring nuclear weapons or fissile materials generally can be thought of as either cooperative or deterrence-based. The Global Threat Reduction Initiative (GTRI) and the Cooperative Threat Reduction (CTR) Program are just two examples of cooperative programs designed, ultimately, to reduce the threat of nuclear materials falling into the wrong hands.⁶ Deterrence-based strategies might apply to those states not as keenly interested in securing their nuclear materials or weapons, or that may even be sponsors of terrorism. The ability to hold a state accountable for either willful or negligent nuclear transfer, realized via post-

³ See Sara Daly, John Parachini, and William Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism* (Santa Monica, CA: RAND Corporation, 2005) for an assessment of the continuing threat.

⁴ Matthew Bunn and Anthony Wier, “Terrorist Nuclear Weapon Construction: How Difficult?” *Annals of the American Academy of Political and Social Science* 607 (September 2006): 136–137.

⁵ Graham Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (New York, NY: Times Books, Henry Holt and Company, LLC, 2004), 140.

⁶ See U.S. Department of Energy, “National Nuclear Security Administration—Office of Global Threat Reduction,” http://nnsa.energy.gov/nuclear_nonproliferation/1550.htm; U.S. Department of Defense, “Cooperative Threat Reduction,” <http://www.dtra.mil/oe/ctr/index.cfm> for more information on these programs.

detonation attribution, is believed to provide a valuable deterrent. Nuclear forensic science purports to make post-detonation attribution possible, thus enabling the desired deterrent posture.

2. Problems and Hypothesis

The United States is currently relying on the science of nuclear forensics to provide a post-detonation attribution capability. Based upon such a capability, the government has at times adopted an explicit deterrent stance. The 2006 National Strategy for Combating Terrorism states, “we will ensure that our capacity to determine the source of any attack is well-known, and that our determination to respond overwhelmingly to any attack is never in doubt.”⁷ Consider, in light of this strategic component, then-President George W. Bush’s carefully worded statement following North Korea’s nuclear test in 2006: “The transfer of nuclear weapons or material by North Korea to states or non-state entities would be considered a grave threat to the United States, and we would hold North Korea fully accountable [for] the consequences of such action.”⁸ The credibility of the deterrent threat rests largely on the U.S. government’s “capacity” to attribute such a transfer to North Korea; a capacity that, in the president’s statement, was only ambiguously implied. Indeed, if the capability is less than perfect, deterrence suffers.

The government itself seemingly acknowledges a less than stellar capability. The 2006 National Strategy for Combating Terrorism also declares, seemingly contradicting the above-cited excerpt, that “We will develop the capability to assign responsibility for the intended or actual use of WMD via accurate attribution—the rapid fusion of technical forensic data with intelligence and law enforcement information.”⁹ Substituting the word “improve” for the word “develop” would have gone further toward “[ensuring] that our capacity to determine the source of any attack is well-known.”¹⁰ Instead the declaration

⁷ Office of the President, *National Strategy for Combating Terrorism*, 14.

⁸ Matthew Phillips, “Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution,” *Orbis* 51, no. 3 (2007): 441.

⁹ Office of the President, *National Strategy for Combating Terrorism*, 15.

¹⁰ *Ibid.*, 14.

is, in effect, a tacit admission of any such capability's nascence. As of October 2009, the U.S. Senate is considering HR 730, the "Nuclear Forensics and Attribution Act," the stated purpose of which is "To strengthen efforts in the Department of Homeland Security to develop nuclear forensics capabilities to permit attribution of the source of nuclear material, and for other purposes."¹¹ These clues, when taken together, indicate the government might, in reality, be scrambling to develop a capability upon which a critical part of its strategy rests and which it has perhaps prematurely implied it possesses.

This potential gap between policy and the capabilities underlying that policy warrants further exploration. Many implications and further questions will arise. In determining what it would take to "close the gap" between reality and desire, I will attempt to estimate the financial, opportunity, and political-capital costs at stake. These costs should be considered against a genuine assessment of the threat, as well as against the potential deterrent benefits derived from spending them on developing a nuclear-forensics-based attribution capability. The discussion should inform the degree of urgency with which the government should proceed.

3. Program Origins and Current Organization

The science of nuclear forensics was first called upon, in an investigative capacity, as part of the intense U.S. effort to detect and analyze early Soviet nuclear activity; in fact, the United States deployed an interim detection network only months prior to the first Soviet atomic weapon test in 1949.¹² Throughout the Cold War, the government sources behind nuclear detonations were generally not in doubt; therefore, post-detonation forensic investigations focused primarily on determining weapon type and design characteristics. Since the 1990s, with the end of the Cold War and a perceived rise in the risk of nuclear terrorism, the aim of nuclear forensic investigations has shifted: the ultimate goal has become the identification of the origins (and the

¹¹ U.S. Congress, "H.R. 730—Nuclear Forensics and Attribution Act," <http://thomas.loc.gov/cgi-bin/bdquery/z?d111:HR730>.

¹² Jeffrey T. Richelson, *Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea* (New York, NY: W. W. Norton & Company, Inc., 2007), 88–94.

originators) of nuclear materials and/or weapons. Although the science itself has not changed substantially over time, this need to *attribute* a nuclear explosion to its source has increased the complexity of the investigative process significantly. In response to this need, the U.S. government has designed its attribution program to harness strengths and skill sets found across the interagency.

Many different government agencies share responsibility for nuclear forensics-based attribution. In the event of a terrorist nuclear attack, the FBI would direct the overall investigation, coordinating the efforts of many supporting actors.¹³ The Department of Defense has recently fielded a Domestic Nuclear Event Attribution (DNEA) team under the auspices of the Defense Threat Reduction Agency (DTRA); this team is prepared to gather evidence via numerous methods and transport this evidence for analysis.¹⁴ Several Department of Energy national laboratories participate in the analysis of collected pre- and post-detonation evidence. The Department of Homeland Security's National Technical Nuclear Forensics Center (NTNFC) serves as a day-to-day focal point for overall interagency nuclear forensics planning and coordination. The Intelligence Community (IC) contributes by sharing information that could strengthen an attribution case; conversely, the IC receives any information resulting from forensic analysis that may focus intelligence-gathering efforts. Each of these agencies, among others, plays an important role in program development, actual attribution operations, or both.

C. LITERATURE REVIEW

I rely on a broad cross-section of literature in assessing the risk of nuclear terrorism, exploring the role of post-detonation nuclear forensics as it bolsters an attribution capability, assessing the current state of that capability, studying the deterrent postures so enabled, and determining the need for further investment based upon threat

¹³ For a more detailed account of the primary actors and their roles, see Joint Working Group of the American Physical Society and the American Association for the Advancement of Science, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 2008, <http://cstsp.aaas.org/files/Complete.pdf>, 36–38.

¹⁴ William J. Broad, “New Team Plans to Identify Nuclear Attackers,” *The New York Times*, February 2, 2006, <http://query.nytimes.com/gst/fullpage.html?res=9E01E0DA1F3FF931A35751C0A9609C8B63&sec=&spoon=&pagewanted=all>.

and theory. Much has been written, ranging from highly technical scientific textbooks to academic policy analysis and advocacy, and there is no broad consensus among scholars on these issues. I will endeavor, therefore, to highlight the strengths and weaknesses of the major arguments as I analyze them, and conclude with appropriate policy recommendations based upon my analysis. Since I have organized my thesis to include literature review throughout, I reserve a detailed analysis of the literature for subsequent chapters.

The literature shows that the argument for or against more investment in a national nuclear forensics-based attribution capability cannot be separated from a thorough analysis of the risk level. Most scholars perceive the risk as either extremely high or extremely low. The risk level, in turn, is partially related to the availability of attribution-enabled deterrence. Policymakers must decide what type of deterrence posture they desire, a decision that should be informed by the attainability of a sufficient attribution capability. The literature delineates the requirements for building and sustaining a credible attribution capability, as well as reveals gaps in the nation's current efforts. A thorough exploration of the body of knowledge on the subject should generate valuable policy recommendations. Ultimately, before assessing if the United States is, in fact, "on target," I will make an informed recommendation as to what the target capability should be.

D. METHODOLOGY

I will take a policy analysis approach to the problem, utilizing a series of literature reviews and relying on several case studies before accepting certain findings as valid and making appropriate policy recommendations. Literature reviews will be accomplished to determine leading schools of thought as to the threat level as well as the application of deterrence. I will briefly explore scientific literature in order to explain the science behind post-detonation nuclear forensics and present an expected timeline for post-attack results. I will also accomplish a literature review to determine the prevailing consensus as to program needs and current capabilities. Existing case studies analyzing recent intelligence and attribution successes and failures will be briefly explored to reveal

potential limitations in current support capability. In order to make a general assessment of the financial costs involved in achieving a more robust forensics program, I will rely on government documents and other sources from which appropriate unclassified budget information can be obtained.

E. THESIS OVERVIEW

This thesis contains five chapters. This opening chapter introduces the thesis topic and research questions, identifies the importance of the research, and addresses certain existing problems in policy and capability. The second chapter reviews leading literature on the threat itself before drawing conclusions as to the degree of alarm with which the nation needs to address this problem. The third chapter reviews literature on the deterrence posture that an attribution capability enables, how such a posture might be employed, and to what effect. Here I will also assess the degree of certainty in an attribution capability required for effective deterrence. This chapter provides a general qualitative estimate of the benefits derived from having such an ability to deter. The fourth chapter provides a layman's technical overview of post-detonation nuclear forensics with a likely timeline for information provision, before reviewing leading literature identifying scientific and supporting requirements for an attribution capability and assessing current U.S. ability to meet those requirements. This chapter concludes with a general qualitative cost estimate for meeting and maintaining such a capability, to include fiscal, opportunity, and political-capital expenditures. Finally, the fifth and concluding chapter presents a summary of findings and makes overall policy recommendations. The next section briefly previews the main findings.

F. FINDINGS

As nuclear terrorism is a risk of low probability and high consequences, the United States is right to address it as a significant—but not the utmost—national security priority. The science of nuclear forensics makes possible the characterization of nuclear materials used in a nuclear attack, and, as such, provides the backbone of an attribution program. Nuclear forensics-based attribution serves the dual purpose of helping to

prevent nuclear terrorism by enabling deterrence, as well as guiding and enabling post-attack response options in the event of deterrence failure. The deterrence that an attribution capability alone enables is fairly narrow in its effective scope, though this deterrence does cover what would otherwise be a critical gap in U.S. strategy for preventing nuclear terrorism. The U.S. attribution capability is currently lacking in several important regards, the most significant of which is a future dearth of highly qualified personnel. Since an attribution capability is a critical enabler, the United States must do more to efficiently develop its attribution program. This can be done most cost-effectively in the short term by focusing on unilateral program needs while building an enduring domestic political will to improve and then maintain the nation's attribution capability.

II. ASSESSING THE THREAT OF NUCLEAR TERRORISM

Is nuclear terrorism something so unlikely that it can be dismissed without much concern and left to novelists and screenwriters as a fear-inspiring plot line? Or is a terrorist nuclear detonation likely to occur within the next ten years, as some analysts predict?¹⁵ Judging from the nature of certain government programs designed to reduce the probability of nuclear terrorism, U.S. policymakers believe it falls somewhere between the two extremes. A correct risk assessment should directly inform measures designed and implemented to reduce this risk. In this chapter, I assess the risk of nuclear terrorism and provide an overview of current U.S. efforts to mitigate this risk. I place attribution-enabled deterrence of state sponsorship in its strategic context, ultimately assessing the importance of the program to the nation's overall risk-mitigation effort. I find that the risk of nuclear terrorism indeed falls somewhere between the two extremes. Additionally, although the U.S. government wisely addresses the entire risk spectrum in its efforts to prevent nuclear terrorism, some of the best opportunities for risk mitigation are found in targeting terrorist capability; attribution-enabled deterrence is uniquely important in this regard.

Determining the correct allocation of scarce and valuable resources for reducing the risk of a terrorist nuclear attack requires a thorough assessment of that risk. The risk of nuclear terrorism must be analyzed based upon the consequences of an attack and the probability of its occurrence. I here use the fairly common definition of risk as a product of probability and consequences ($R=P \times C$), where the probability (P) of an event is affected by the nature of the threat (T) and the vulnerability (V) of the system in question ($P=T \times V$). Although I will not quantitatively utilize this formula, it does provide a valuable framework with which to qualitatively analyze the problem.

¹⁵ Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1–120; Bob Graham et al., *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (New York, NY: Vintage Books, 2008), xv.

I begin the risk assessment by reviewing literature from leading scholars reflecting their overall views of the risk of nuclear terrorism.¹⁶ I then briefly describe the potential consequences of a terrorist nuclear attack, before moving to a longer discussion of probability on the basis of the threat and U.S. vulnerability to attack. I conclude the chapter with an analysis of current risk mitigation efforts.

A. OVERALL ASSESSMENTS OF THE RISK

Most academic work on nuclear terrorism acknowledges the severity of the potential consequences of a terrorist nuclear attack, although scholars differ as to its likelihood. Graham Allison devotes the first half of his book, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, to a grim assessment of this risk.¹⁷ He maintains that, given the U.S. government's current approach to the problem, such an attack is "more likely than not."¹⁸ Micah Zenko reviews declassified national intelligence estimates covering the past fifty years before concluding that the possibility of a nuclear terrorist attack is very real, and that the government has been sufficiently warned.¹⁹ Matthew Bunn develops and applies a model which creates a quantitative result, leading to his conclusion that there is a "29% probability of a nuclear terrorist attack in the next decade."²⁰ Although these scholars share a similar sense of alarm about the risk, others perceive it very differently.

While acknowledging the enormous potential consequences of nuclear terrorism, some scholars present a more moderate viewpoint on its likelihood. John Parachini relies on the sparse case studies that are found in the historical record of terrorist use of WMD

¹⁶ Nuclear terrorism in this thesis indicates a terrorist detonation of a device producing actual nuclear yield. This usage excludes the detonation of a Radiological Dispersal Device (RDD), sabotage using radiological materials, or attacks on existing nuclear facilities; it includes terrorist detonation of either state-produced nuclear weapons or terrorist-built Improvised Nuclear Devices (INDs). The discussion is thus limited to the most consequential form of terrorist nuclear attack.

¹⁷ Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1–120.

¹⁸ Ibid., 15.

¹⁹ Micah Zenko, "Intelligence Estimates of Nuclear Terrorism," *Annals of the American Academy of Political and Social Science* 607 (September 2006): 87–102.

²⁰ Matthew Bunn, "A Mathematical Model of the Risk of Nuclear Terrorism," *Annals of the American Academy of Political and Social Science* 607 (September 2006): 103.

to conclude that a combination of technical factors, opportunity, and leadership mindset all overwhelmingly lessen the risk.²¹ Jessica Stern offers technical, motivational, and organizational constraints on terrorist use of nuclear weapons while concluding that the probability of such an attack is extremely low.²² Robin Frost argues that “the risk of nuclear terrorism ... is overstated,” justifying his view on technical, psychological, and strategic grounds.²³ Frost sets out to discredit assumptions regarding the existence of a thriving international black market for nuclear weapons and materials, the ease of building a nuclear weapon once the material is in hand, and the likelihood that a “rogue” state might hand a nuclear weapon to a terrorist group, among others.²⁴ Brian Jenkins sees nuclear terrorism as unlikely, arguing that policies in response to sensationalism are detrimental to U.S. national security.²⁵ John Mueller includes nuclear terrorism in his list of “inflated” national security threats.²⁶ All of these scholars, no matter where they fall on the “sense-of-alarm” scale, focus on several challenging prerequisites to nuclear capability in making their cases. After describing the consequences of a terrorist nuclear attack, I explore both the intent and capability of terrorist groups before assessing the nation’s current vulnerability.

B. RISK COMPONENTS

1. Consequences

In a worst-case scenario, the consequences of a terrorist nuclear attack would be horrific. An IND might achieve yields of up to several kilotons, and, if detonated in the center of a city, could kill hundreds of thousands of people and cause direct physical

²¹ John Parachini, “Putting WMD Terrorism into Perspective,” *The Washington Quarterly* 26 (Autumn 2003): 42–46.

²² Jessica Stern, *The Ultimate Terrorists* (Cambridge, MA: Harvard University Press, 1999), 10, 48–86.

²³ Robin Frost, “Nuclear Terrorism after 9/11,” *Adelphi Papers* 45, no. 378 (2005): 7.

²⁴ *Ibid.*, 8–10.

²⁵ Brian Michael Jenkins, *Will Terrorists Go Nuclear?* (Amherst, NY: Prometheus Books, 2008).

²⁶ John Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why we Believe them* (New York, NY: Free Press, 2006), 14–17.

damage ranging into hundreds of billions of dollars.²⁷ The long-term economic and health consequences from elevated radiation levels would be severe.²⁸ Similar follow-on attacks would almost certainly be threatened, resulting in panic and devastating the international economy.²⁹ Since this scenario would be unimaginably devastating, the consequences (C) component of the risk equation ($R=P \times C$) is extremely high.³⁰ Risk, then, varies with probability in this case. If the probability is determined to be greater than zero, risk will be proportionately high. Available measures for reducing probability must be weighed against their cost, as well as policymakers' and the public's tolerance for such risk. Before assessing measures for reducing the probability of terrorist nuclear attack, the intentions and capabilities of potential adversaries as well as system vulnerabilities must be considered.

2. Probability—Intent

Determining an adversary's intent is sufficiently difficult when one's adversary is a state. The problem is further complicated when the adversary is a non-state actor. Although scholars disagree on the seriousness with which terrorist groups have and may continue to pursue nuclear weapons, as well as their intent to utilize nuclear weapons should they obtain them, a certain level of intent does exist and cannot be dismissed. Al Qaeda has declared its intent to pursue WMD, obtained a fatwa approving the use of such

²⁷ Graham Allison, "Nuclear Deterrence in the Age of Nuclear Terrorism," *Technology Review* 111, no. 6 (November/December 2008): 71.

²⁸ Ashton B. Carter et al., *The Day After: Action in the 24 Hours following a Nuclear Blast in an American City* (Cambridge, MA: Preventive Defense Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2007), http://belfercenter.ksg.harvard.edu/publication/2140/day_after.html, 5–6.

²⁹ Matthew Bunn, *The Risk of Nuclear Terrorism - and Next Steps to Reduce the Danger*, Written Testimony before U.S. Senate Committee on Homeland Security and Governmental Affairs, April 2, 2008, <http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=42449878-5e68-4eef-978d-8e671fed2ab0>, 5.

³⁰ Not all scholars share this worst-case assumption. I argue that regardless of first-order consequences, second- and third-order effects from a terrorist nuclear detonation would almost certainly be severe enough to cause major international upheaval; as such, I assign a qualitatively high value to C in my risk equation. For an interesting discussion of nuclear-weapon-effects modeling and recommendations for preventing the most severe consequences, see Robert C. Harney, "Inaccurate Prediction of Nuclear Weapons Effects and Possible Adverse Influences on Nuclear Terrorism Preparedness," *Homeland Security Affairs* 5, no. 3 (September 2009), <http://www.hsaj.org/?article=5.3.3>.

weapons, and “justified” the killing of four million Americans.³¹ Aum Shinrikyo’s founder was obsessed with obtaining nuclear weapons for the purpose of catalyzing “Armageddon.”³² Although Aum Shinrikyo’s founder is in prison and Al Qaeda’s nuclear focus may have waned, the intentions of these and other terrorist organizations and individuals are and will continue to be exceedingly difficult to determine with any precision. The safe and conservative approach, and the one I adopt here, is to assume a continuing serious intent on the part of terrorist organizations to obtain and use nuclear weapons.³³ Real or assumed serious intentions notwithstanding, all non-state actors face the same set of very real and difficult obstacles to achieving a nuclear capability.

3. Probability—Capability

States alone are realistically capable of manufacturing the Special Nuclear Material (SNM)³⁴ necessary for nuclear weapons; therefore, terrorists are left to beg, borrow, steal, or otherwise be entrusted by a state with HEU, plutonium, or an entire weapon itself.³⁵ These avenues to obtaining either SNM or nuclear weapons can be broken down into several categories for analysis: theft from state stockpiles, black market purchase, and purposeful state transfer to terrorists.

³¹ Rolf Mowatt-Larssen, *Nuclear Terrorism: Assessing the Threat to the Homeland*. Written Testimony before U.S. Senate Committee on Homeland Security and Governmental Affairs, April 2, 2008, <http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=42449878-5e68-4eef-978d-8e671fed2ab0>.

³² Daly et al., *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism*, 5–9.

³³ Although a distinction may be made between the intent to acquire and the intent to use nuclear weapons, I here make the assumption that a terrorist organization which acquires a nuclear weapon intends to use it. If terrorists can be prevented from acquiring a nuclear capability, questions of their intent to use nuclear weapons become moot. As such, by taking advantage of reasonable opportunities to prevent terrorist acquisition of nuclear weapons, the United States does more to reduce the risk of nuclear terrorism than by relying on the uncertain deterrence of a nuclear-armed terrorist group. For analyses of the possibility of deterring nuclear-armed terrorists, see Lewis A. Dunn, “Can Al Qaeda be Deterred from Using Nuclear Weapons?” in *Weapons of Mass Destruction and Terrorism*, 295–316; David P. Auerswald, “Deterring Nonstate WMD Attacks,” *Political Science Quarterly* 121, no. 4 (Winter 2006/2007): 543–568.

³⁴ Special Nuclear Material (SNM), as defined by the Atomic Energy Act of 1954, refers to plutonium (Pu), uranium-233, or uranium (U) enriched with U-233 or U-235. This includes both Low-Enriched Uranium (LEU), uranium enriched to less than 20% U-235, as well as Highly-Enriched Uranium (HEU), uranium enriched to 20% or greater U-235. Uranium is considered weapons-grade when it has been enriched to 90% or greater U-235.

³⁵ Bunn and Wier, “Terrorist Nuclear Weapon Construction: How Difficult?” 136–137.

Purposeful state transfer of a nuclear weapon is the most improbable scenario. Frost implies that the most compelling reason for a state not to share nuclear weapons with terrorists is simply that the state could not guarantee the weapons would not be used against itself.³⁶ Further, he suggests that for lesser-power states, nuclear weapons are valued as a national treasure and would therefore be carefully guarded and not given away.³⁷ Robert Jervis is another author who shares Frost's conclusions, and adds—using the case of Saddam Hussein and Iraq—that it was not clear how sponsoring a terrorist attack on the United States would further any state objectives.³⁸ Lebovic suggests that scholars have “[failed] to indicate what an adversary could gain from a nonconventional weapons attack.”³⁹ For these same reasons, terrorist theft of a nuclear weapon, as well as the availability of an entire nuclear weapon on the black market, both are highly unlikely. States treat nuclear weapons as matters of the utmost national security, and are unlikely to relinquish control over them, purposefully or not.

One notable “loophole” in states’ airtight security over nuclear weapons might come in the form of unstable regimes with nuclear weapons. Much attention has recently been given to Pakistan and its nuclear arsenal of some 50 weapons. With increasing unrest fomented by Islamic extremists, and with Taliban fighters recently advancing to within 60 miles of Islamabad, the Pakistani government has repeatedly reassured the United States that its nuclear arsenal is secure.⁴⁰ Even if the worst case was realized and extremists took control of Pakistan’s nuclear arsenal, one cannot assume they would transfer nuclear weapons to terrorists or otherwise initiate a nuclear attack by proxy. Certain scholars believe that even the most extreme regimes can be deterred from using

³⁶ Frost, “Nuclear Terrorism after 9/11,” 64.

³⁷ Ibid.

³⁸ Robert L. Jervis, “The Confrontation between Iraq and the U.S.: Implications for the Theory and Practice of Deterrence,” *European Journal of International Relations* 9, no. 2 (2003): 332.

³⁹ James H. Lebovic, *Deterring International Terrorism and Rogue States: U.S. National Security Policy after 9/11* (New York, NY: Routledge, 2007), 30.

⁴⁰ David E. Sanger, “Strife in Pakistan Raises U.S. Doubts over Nuclear Arms,” *New York Times*, May 4, 2009, http://www.nytimes.com/2009/05/04/world/asia/04nuke.html?_r=1&scp=1&sq=pakistan nuclear may 4 2009&st=cse.

or transferring nuclear weapons.⁴¹ As Lebovic simply states, “even the irrational can consider costs.”⁴² Here I point out an important caveat—this logic assumes the existence of a deterrent posture, which, in turn, requires the ability to determine the source of a terrorist nuclear attack. However unlikely, an “irrational,” extremist-run state might transfer a nuclear weapon to terrorist proxies if it believed such a transfer would remain undetected.⁴³ This is an important area in which the risk of nuclear terrorism is only reduced with the existence of an attribution-enabled deterrence capability.

Terrorists groups, failing to obtain a functional nuclear weapon, may attempt to procure the necessary SNM to build one of their own. Terrorist groups might attempt to steal SNM from state sources or seek to buy it on the black market. Nothing in open-source literature indicates that terrorists have attempted to steal SNM. However, the criminal infiltration of a South African nuclear facility in 2007 exposes the feasibility of such thievery.⁴⁴ Al Qaeda has made several serious attempts over many years to purchase SNM on the black market, with several notable failures and no known successes.⁴⁵ In spite of vast resources and connections, Aum Shinrikyo was unable to obtain weapons or SNM and turned instead to uranium mining and enrichment in its nuclear quest—a quest that was ultimately a failure.⁴⁶ These past terrorist attempts and failures to obtain SNM indicate the degree to which the supply side has failed to meet the demand side, which a brief look at the historical nature of the black market itself confirms.

⁴¹ See Kenneth Waltz and John Mearsheimer as quoted in Bennett, Drake, “Give Nukes a Chance: Can the Spread of Nuclear Weapons make U.S. Safer?” *The Boston Globe*, March 20, 2005, http://www.boston.com/news/globe/ideas/articles/2005/03/20/give_nukes_a_chance/, 30.

⁴² Lebovic, *Deterring International Terrorism and Rogue States: U.S. National Security Policy after 9/11*, 30.

⁴³ Jeffrey W. Knopf, “Deterrence or Preemption?” *Current History* 105, no. 694 (November 2006): 398.

⁴⁴ Bunn, *The Risk of Nuclear Terrorism—and Next Steps to Reduce the Danger*, 1.

⁴⁵ Daly et al., *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism*, 28–33.

⁴⁶ *Ibid.*, 18–21.

Since the breakup of the Soviet Union in 1991, the IAEA has confirmed only twenty cases of trafficking in either HEU or plutonium.⁴⁷ None of these have involved more than a very small fraction of the material needed to produce a nuclear weapon, and the amount actually involving weapons-grade material is debatable.⁴⁸ Open-source intelligence indicates a paucity of credible sellers, with scam artists and desperate thieves abounding.⁴⁹ By itself, this lack of evidence regarding “successful” black market transfers to terrorists does not preclude a successful transfer of substantial fissile material in the future; however, there are no indications that black market conditions have become more dangerous. The paucity of evidence also does not guarantee that a past transfer has not occurred. Even if a transfer has occurred—or does occur in the future—the next step toward achieving a nuclear capability is daunting.

Let us assume, for the sake of argument, that a terrorist organization was able to obtain SNM. Would they be able to build a bomb producing nuclear yield? There are several formidable obstacles. First, approximately eight kilograms of plutonium, or 25 kilograms of HEU, is required to build a crude nuclear weapon.⁵⁰ As alluded to above, known black market transactions have involved substantially smaller amounts. The largest was approximately 1/8th what is required.⁵¹ For a number of technical reasons, HEU would provide a terrorist organization a more likely path toward success than plutonium.⁵²

Once in possession of a sufficient quantity of weapons-grade HEU, a terrorist organization would likely select a “gun-type” design for their nuclear device. This, the simplest design, involves the use of conventional explosives to force two subcritical

⁴⁷ Frost, “Nuclear Terrorism after 9/11,” 13.

⁴⁸ Ibid.

⁴⁹ Ibid., 16–17.

⁵⁰ Charles D. Ferguson and William C. Potter, *The Four Faces of Nuclear Terrorism* (Monterey, CA: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004), 106.

⁵¹ Frost, “Nuclear Terrorism after 9/11,” 14.

⁵² Robert L. Gallucci, “Averting Nuclear Catastrophe: Contemplating Extreme Responses to U.S. Vulnerability,” *Annals of the American Academy of Political and Social Science* 607 (September 2006): 52.

masses of HEU together at high speed, forming a supercritical mass with nuclear yield.⁵³ Scientists' confidence in this simple and robust design was so high that it was not tested prior to its deployment over Hiroshima in 1945.⁵⁴ However, a rudimentary understanding of the weapon design only serves as a starting point. The HEU must be in the correct form, portioned and machined with a certain degree of precision. The "gun" must be loaded with the correct amount of conventional explosives, and a trigger mechanism installed. Such technical difficulties, among others, belie any suggestions regarding ease of construction. However, seized documents indicate Al Qaeda has received informational support regarding nuclear-weapons design and fabrication from Pakistani scientists on at least one occasion.⁵⁵ Moreover, given Al Qaeda's expertise and experience in designing and building Improvised Explosive Devices (IEDs), its ability to assemble the right team of conventional-explosive experts cannot be dismissed. Thus possessing the right amount of HEU would present a terrorist organization with a feasible, yet still formidable, path to a nuclear weapon.

Though significantly less plutonium than HEU is required for a nuclear weapon, plutonium-based nuclear weapon construction is more difficult for a number of reasons. First, plutonium is more radioactive than uranium; as such, it is more easily detected and must be more carefully handled. Plutonium, created through the fission process in a nuclear reactor, is not usable while still trapped in spent fuel—it must be separated. Once separated, it is technically usable for weapons whether it is reactor-grade or weapons-grade.⁵⁶ However, making use of non-weapons grade plutonium as well as plutonium in oxide form would require larger quantities of the plutonium and a higher degree of technical sophistication.⁵⁷ Moreover, plutonium cannot be used in a "gun-type" weapon,

⁵³ Bunn and Wier, "Terrorist Nuclear Weapon Construction: How Difficult?," 139–140.

⁵⁴ Gallucci, "Averting Nuclear Catastrophe: Contemplating Extreme Responses to U.S. Vulnerability," 52.

⁵⁵ David. Albright, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents," Nautilus Institute Policy Forum Online, Special Forum 47 (November 6, 2002), http://www.nautilus.org/archives/fora/Special-Policy-Forum/47_Albright.html.

⁵⁶ Bunn and Wier, "Terrorist Nuclear Weapon Construction: How Difficult?," 136.

⁵⁷ Ibid.

but must be utilized in a more complex “implosion-type” design.⁵⁸ An implosion-type weapon requires an almost-perfectly-simultaneous conventional explosion around an inner almost-perfectly-shaped plutonium core in order to begin the fission chain reaction.⁵⁹ Determining the required amount of compression is usually done through sophisticated testing; this would be difficult for any terrorist organization to accomplish absent ample sanctuary and the associated feedback equipment. In short, although creating a nuclear weapon is technically possible once the correct amount and type of plutonium is in hand, it would be a daunting prospect for any terrorist organization.

As I have shown, there are several means by which a terrorist organization could acquire nuclear capability; some of these means are less likely than others. States are highly unlikely to purposefully transfer nuclear weapons or materials to terrorists. The probability of purposeful state transfer can be further reduced with a credible deterrent posture. Terrorist theft of a nuclear weapon is even more unlikely than purposeful state transfer. Terrorists have not demonstrated the intent to steal SNM, though such a scenario seems entirely plausible. The black market for SNM has failed to produce quantities sufficient for a nuclear weapon, and, further, has failed to unite credible terrorist demand with supply. Even if terrorists did manage to somehow obtain sufficient SNM for a weapon, constructing a functional nuclear device is by no means a sure thing, much less so for plutonium-based versus HEU-based devices. Taken together, even assuming a significant intent on the part of terrorist organizations, these formidable obstacles to achieving nuclear capability indicate a very low threat (T) component for nuclear terrorism.

4. Probability—Vulnerability

To carry out a nuclear attack on the United States, terrorists would either have to:
1) obtain, in the United States, a nuclear weapon or SNM; or, 2) smuggle a weapon or

⁵⁸ Bunn and Wier, “Terrorist Nuclear Weapon Construction: How Difficult?,” 140.

⁵⁹ Ibid., 140–142.

SNM into the United States or at least as far as one of its ports.⁶⁰ As long as either of these two avenues is available, the United States will be vulnerable to nuclear terrorism. Since any given state cannot absolutely control what passes over its borders, vulnerability cannot be reduced to zero. However, means for reducing this vulnerability should become evident from a closer look at each concern.

Could terrorists really obtain SNM or even a nuclear weapon here in the United States? Such a thought would have been incredible prior to August 30, 2007. On that day, a United States Air Force B-52 bomber flew from North Dakota to Louisiana with six nuclear-armed cruise missiles on the rails under its wings, a mistake not discovered until ten hours after landing.⁶¹ In essence, the United States could not account for six nuclear warheads for the better part of a day. Congressman Edward Markey said it best: “The complete breakdown of the Air Force command and control over enough nuclear weapons to destroy several cities has frightening implications not only for the Air Force, but for the security of our entire nuclear weapons stockpile.”⁶² Indeed, this incident brings to the forefront questions about the security of not just nuclear weapons, but also the nation’s SNM stockpiles.

As of 2003, the United States possessed approximately 100 metric tons of plutonium and 600 metric tons of HEU.⁶³ Matthew Bunn points out several ways in which security of SNM at U.S. sites is deficient and could be improved.⁶⁴ Among them, U.S. research reactors using HEU are exempt from the stringent security rules to which commercial reactors are subject.⁶⁵ The B-52 incident and these few security deficiencies

⁶⁰ The likelihood that terrorists would obtain any other means for nuclear delivery, e.g., bomber or missile, is so low as to be negligible.

⁶¹ Josh White, “In Error, B-52 Flew over U.S. with Nuclear-Armed Missiles,” September 6, 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/05/AR2007090500762.html>.

⁶² Ibid.

⁶³ David Albright and Kimberly Kramer, “Fissile Material: Stockpiles Still Growing,” *Bulletin of the Atomic Scientists* 60, no. 6 (November/December 2004): 15, http://www.isis-online.org/global_stocks/bulletin_albright_kramer.pdf.

⁶⁴ Matthew Bunn, *Securing the Bomb 2008* (Cambridge, MA: Project on Managing the Atom, Harvard University and Nuclear Threat Initiative, 2008), 181–182.

⁶⁵ Ibid.

notwithstanding, terrorists would likely have an easier time procuring SNM or a weapon outside of the United States.⁶⁶ Could either be smuggled across U.S. borders?

Given an adversary with sufficient determination and resources, the unfortunate answer is “yes.” The amount of plutonium or uranium required to build a crude nuclear weapon could easily fit into a one-gallon container.⁶⁷ Highly enriched uranium emits very little harmful radiation, and plutonium can be shielded for safe handling.⁶⁸ Since the United States shares thousands of miles of remote and relatively porous borderland with Mexico and Canada, crossing undetected with SNM might be done over land or water with a minimal support network and related footprint.

Conversely, an assembled weapon would almost certainly have to transit a land or sea border point due to its large size. A major vulnerability is simply the inability to perform a detailed search of the millions of shipping containers entering the nation each year. Additionally, the proximity of the six major U.S. maritime ports to major metropolitan areas leaves thousands of people within range of a nuclear detonation before the weapon actually crosses the border. Thus, although difficult to quantify, in light of the above-described deficiencies I find U.S. vulnerability to nuclear terrorism to be generally high. I address certain U.S. government programs and policies designed to reduce these vulnerabilities in the next section, which will place these measures in the context of efforts to mitigate the overall risk of nuclear terrorism.

C. CURRENT MITIGATION EFFORTS

Because of the relationship between threat, vulnerability, and probability ($P=T \times V$), a very low threat component yields a correspondingly low probability. Though the probability of nuclear terrorism is very low, it is not zero. Recall the equation relating probability and consequences to risk ($R=P \times C$). As the probability of occurrence approaches zero, risk is rapidly reduced. If the probability is zero, there is no risk. As the consequences of a nuclear detonation in a city are undoubtedly severe, those who

⁶⁶ Matthew Bunn, *Securing the Bomb* 2008, 7.

⁶⁷ Bunn and Wier, “Terrorist Nuclear Weapon Construction: How Difficult?” 140.

⁶⁸ *Ibid.*, 135–136.

would dismiss the risk of nuclear terrorism as “overblown” are assuming, either implicitly or not, that the probability is so small as to be virtually zero. Since the probability of a terrorist nuclear attack is greater than zero, the risk of nuclear terrorism is present, and, due to the horrific consequences of such an attack, cannot be dismissed. Important steps are being taken to reduce this risk. These steps focus on both the threat—the intent and capability of terrorist groups—and the nation’s vulnerability.

The U.S. government, in partnership with other nations, is executing a multifaceted strategy for reducing the risk of nuclear terrorism. The U.S. and other governments target the intent of Islamic terrorist groups by encouraging the spread of messages that lessen the appeal of nuclear weapons. Many widely respected Imams have discredited nuclear weapons in general.⁶⁹ These and similar messages may be effective at reducing the desire for nuclear weapons among terrorist groups depending on the support of a broad constituency; however, “doomsday” terrorist groups hoping to achieve “Armageddon” would likely be unfazed at such public opinion.⁷⁰

The United States also targets the intent of terrorist groups via deterrence. Some aspects of this deterrence fall under what Glenn Snyder called “deterrence by denial.”⁷¹ Such deterrence is achieved by creating barriers that make a successful attack less likely, as well as by reducing the potential gains of a successful attack.⁷² Barriers to a successful attack include radiation detectors and other forms of cargo screening at U.S. ports of entry, as well as interdiction efforts targeting nuclear-materials trafficking worldwide.⁷³ The government is taking steps to bolster response and recovery plans,

⁶⁹ Garfinkle, “Does Nuclear Deterrence Apply in the Age of Terrorism?” *Foreign Policy Research Institute Footnotes* 14, no. 10 (May 2009), <http://www.fpri.org/footnotes/1410.200905.garfinkle.nucleardeterrenceterrorism.html>.

⁷⁰ Stern, *The Ultimate Terrorists*, 70–76.

⁷¹ Glenn H. Snyder, *Deterrence by Denial and Punishment* (Princeton, NJ: Princeton University Center of International Studies), 1959.

⁷² Snyder illustrates the concept using the defense provided by conventional forces during the Cold War. Caitlan Talmadge makes a more contemporary application in Caitlin Talmadge, “Deterring a Nuclear 9/11,” *The Washington Quarterly* 30, no. 2 (2007): 22–23.

⁷³ For an analysis of challenges inherent in implementing the newest radiation detection technology, see United States Government Accountability Office, *Combating Nuclear Smuggling*; for an overview of the premier international interdiction program see U.S. Department of State, “Proliferation Security Initiative,” <http://www.state.gov/t/isn/c10390.htm>.

training, and capability to help mitigate the consequences of a successful nuclear attack.⁷⁴ These “deterrence by denial” efforts may also be categorized as vulnerability mitigation efforts, and some will be described in greater detail below.

Other deterrence-based intent-mitigating efforts, such as threats of an “overwhelming response” to terrorists following WMD attacks, directly reflect “deterrence by punishment” strategy.⁷⁵ The United States’ ability to dissuade certain terrorist groups from pursuing or using nuclear weapons via promises of retaliatory actions is less than assured. Although such efforts may yield positive results and should be continued, I argue that the most effective, universal measures for reducing the threat of nuclear terrorism focus not on terrorist intent, but capability.

There are multiple ways of targeting the nuclear capability of terrorist groups. The United States has maintained the offensive against Al Qaeda, thus largely denying them the sanctuary required to develop and build a nuclear weapon. The international community has joined in disrupting terrorist finances, limiting funding for black-market purchases and operations in general. Many additional programs and policies more specific to the nuclear threat are in place as well.

The policies and programs utilized to prevent terrorists from acquiring nuclear weapons or SNM generally can be categorized as one of two types—cooperative or deterrence-based.⁷⁶ Several cooperative organizations and regimes have been created or strengthened in an effort to prevent the unintentional transfer of SNM to terrorists. The Cooperative Threat Reduction Program (CTR) has been active since the early 1990s to secure and dismantle nuclear weapons in the former Soviet Union.⁷⁷ The Proliferation Security Initiative (PSI) was launched in 2003 as a voluntary effort among participating

⁷⁴ Homeland Security Council, *National Planning Scenarios: Executive Summaries* (Version 2.0) (Washington, DC, 2004), 1.1–1.5; Carter, et al., *The Day After*, 11. Carter notes that as of 2007, the government was still drafting a comprehensive and realistic response plan.

⁷⁵ Office of the President, *National Strategy for Combating Terrorism*, 14.

⁷⁶ Some coercive efforts do not neatly fit into this general categorization. A distinction between deterrence and compellence is made and discussed in Chapter III.

⁷⁷ U.S. Department of Defense, “Cooperative Threat Reduction,” <http://www.dtra.mil/oe/ctr/index.cfm>.

nations (now more than 90) to stop the trafficking in WMD and related materials.⁷⁸ The PSI uses enhanced information-sharing and cooperation across law enforcement and intelligence boundaries to prevent transactions by arrest and/or interdiction. More recently, in 2006 the Global Threat Reduction Initiative (GTRI) was created, in part, to remove, properly dispose of, or ensure the protection of SNM worldwide.⁷⁹ Although problems remain, these programs work together to decrease the overall likelihood of transfer.

Deterrent strategies have been designed to cover those areas beyond the “reach” of cooperative programs. Potential targets, which will be discussed in detail in Chapter III, might include any semi- and non-cooperative nuclear states, regardless of whether they are known sponsors of terrorism. The United States has proclaimed its “determination to respond overwhelmingly to any [WMD] attack,” and targeted this threat in general at “terrorists and those who aid or sponsor a WMD attack.”⁸⁰ An attribution capability alone provides the basis for such deterrent threats, thus filling what might otherwise be a critical gap in strategy. Importantly, the United States has also anticipated terrorist acquisition of a nuclear capability, whether through deterrence failure or not, and taken steps intended to reduce the nation’s vulnerability.

Vulnerability can be reduced, in part, by preventing SNM or nuclear weapons from reaching and passing through U.S. ports or from otherwise crossing national borders. The Department of Homeland Security’s U.S. Customs and Border Protection (CBP) agency has two major programs in place designed to prevent terrorist weapons or materials from entering the country: the Customs-Trade Partnership Against Terrorism (C-TPAT), and the Container Security Initiative (CSI).

⁷⁸ U.S. Department of State, “Proliferation Security Initiative,” <http://www.state.gov/t/isn/c10390.htm>.

⁷⁹ U.S. Department of Energy, “National Nuclear Security Administration—Office of Global Threat Reduction,” http://nnsa.energy.gov/nuclear_nonproliferation/1550.htm.

⁸⁰ Office of the President, *National Strategy for Combating Terrorism*, 14.

C-TPAT, a public-private sector partnership started in November 2001, has now established links with more than 7,400 companies.⁸¹ This program provides benefits and incentives to member companies, which include expedited shipment processing, in return for improved security along member companies' entire supply chains.⁸² C-TPAT thus establishes a shared responsibility for security from which mutual benefits are derived. However, since participation is voluntary, the security enhancements are not comprehensive. C-TPAT, then, is but one layer of CBP's defense that complements another—the Container Security Initiative.⁸³

CSI is a multinational program designed to identify and pre-screen high-risk shipping containers before they leave foreign ports.⁸⁴ Bilateral agreements allow multi-discipline CBP teams to operate in foreign ports currently covering approximately 85% of the containerized maritime cargo bound for the United States.⁸⁵ Required trade data is used to determine high-risk containers, which are then singled out for either non-intrusive or physical inspection.⁸⁶ Non-intrusive inspection is often accomplished with radiation-detection equipment provided through the National Nuclear Security Administration's "Megaports Initiative."⁸⁷

The four major types of radiation-detection equipment currently in use by the United States each have certain technological limitations that decrease their efficiency; these range from false alarms to simple failure to detect contraband when sufficient background noise is present.⁸⁸ These technological limitations do not seriously impede

⁸¹ U.S. Customs and Border Protection, *Securing the Global Supply Chain: Customs-Trade Partnership Against Terrorism (C-TPAT) Strategic Plan* (Washington, DC: U.S. Customs and Border Protection, 2004), 2.

⁸² *Ibid.*, 7.

⁸³ U.S. Customs and Border Protection, *Container Security Initiative: 2006-2011 Strategic Plan* (Washington, DC: U.S. Customs and Border Protection, 2006), 9.

⁸⁴ *Ibid.*, 4.

⁸⁵ *Ibid.*, 6.

⁸⁶ *Ibid.*, 15–19.

⁸⁷ *Ibid.*, 18; also see U.S. Department of Energy, National Nuclear Security Administration Website, "Megaports Program Coming to Jamaica," <http://nnsa.energy.gov/news/1039.htm>.

⁸⁸ Jonathan Medalia, *Detection of Nuclear Weapons and Materials: Science, Technologies, Observations*. CRS Report R40154 (Washington, DC: Congressional Research Service, 2009), 12.

CBP operations; however, they do leave open certain vulnerability gaps in the nation's borders. The now-unfunded Advanced Spectroscopic Portal and Cargo Advanced Automated Radiography System together promised to fill existing vulnerability gaps in the near term, as well as provide a technological bridge to fill still more in the future.⁸⁹ The research and development for these programs surpassed designated timelines and budgets, and the technology ultimately failed to meet expectations.⁹⁰ In addition to lingering deficiencies at border checkpoints, Senator Joseph Lieberman suggests that avenues for nuclear smuggling such as "general aviation, small-craft maritime activities and unprotected land border areas" are left vulnerable due to the unrealized promise of new technology.⁹¹

This discussion of current risk-mitigation programs illustrates the overall effort the United States is making to reduce the risk of nuclear terrorism, both in terms of terrorist intent and capabilities as well as with regard to national vulnerability to nuclear terrorism. Taken together, these efforts compose a strategic puzzle in which the attribution-enabled deterrence of state sponsorship of nuclear terrorism represents only one piece. However, efforts at reducing national vulnerability or targeting terrorist intent appear to offer less promise for lowering risk than does working to prevent terrorists from acquiring a nuclear capability. Attribution-enabled deterrence fills a critical role in this capability-denying prevention effort.

D. CHAPTER SUMMARY

Overall, the threat component of nuclear terrorism is very low, yet the overall risk remains significant due to the enormous potential consequences of an attack, as well as the relatively high level of U.S. vulnerability to attack. In this chapter, I have provided a detailed risk assessment, demonstrating the importance of individual policies and programs by pointing out what risk-mitigating needs they meet. Risk may be mitigated

⁸⁹ Joseph Lieberman, *Preventing Nuclear Terrorism: Hard Lessons Learned From Troubled Investments?* Chairman's Opening Statement for the U.S. Senate Committee on Homeland Security and Governmental Affairs, September 25, 2008, <http://hsgac.senate.gov/public/files/092508JILOpen.pdf>

⁹⁰ Lieberman, *Preventing Nuclear Terrorism: Hard Lessons Learned from Troubled Investments?*

⁹¹ Ibid.

by lowering the probability or consequences of attack, as well as the nation's vulnerability to attack. I find that reducing the probability of attack by targeting terrorist capability currently offers the best potential results. Several obstacles inherent to the process of obtaining a nuclear capability can be exploited to further lessen the probability that any terrorist group will achieve nuclear "success." For example, though likely reticent in any event to transfer nuclear weapons to terrorists, states can be deterred through a posture enabled by an attribution capability, reducing an already low probability. Additionally, better security for SNM stockpiles around the world will reduce the possibility of theft or black-market availability to terrorists. The United States rightly invests in programs intended to exploit these obstacles.

III. DETERRENCE THEORY

Regardless of the current status of its nuclear forensics-based attribution capability, the United States must determine the appropriate application of the deterrence strategies it might enable.⁹² In this chapter, I will provide a policy-oriented analysis of this aspect of deterrence, first placing it in strategic context and then analyzing it on a theoretical basis. Along the way, I will address questions of whether and to what degree it is possible to deter “rogue” state sponsors of terrorism, and whether a perfect attribution capability is required for effective deterrence or a less-than-perfect capability will suffice. I will explore certain attribution-enabled pre-attack deterrent postures as well as potential post-attack responses. Balancing issues of credibility and effectiveness, I will recommend the deterrent posture the United States should adopt.

As a starting point, I borrow the following useful definition: “deterrence can be defined as the use of threats by one party to convince another party to refrain from initiating some course of action.”⁹³ In analyzing the potential utility of any given strategic initiative that relies on deterrence, each element of this concept must be considered: *Who* wishes to deter *whom* from initiating *precisely what action*, and *how convincing* are these threats?

A. WHO?

At first glance, this seems to be the easiest question to answer—the United States is the actor issuing the deterrent threats in this case. It is important, however, to make some further distinctions in this area. Although the 2006 National Strategy for Combating Terrorism is still in effect, a new presidential administration has come to power. It was President Bush who issued the deterrent threat to North Korea in a 2006

⁹² Michael Levi made this point in testimony before Congress: “Strategy is as important as technology. The United States needs to determine what consequences would follow terrorist attacks, and to communicate these to would-be state sponsors.” As quoted in Charles D. Ferguson, “Can Nuclear Forensics Trace a Detonated Nuclear Weapon to its Source?” Paper prepared for the 2006 Annual Meeting of the American Political Science Association, Philadelphia, PA, August 30–September 3, 2006, 8.

⁹³ Paul K. Huth, “Deterrence and International Conflict: Empirical Findings and Theoretical Debates,” *Annual Review of Political Science* 2 (1999): 26.

speech—does that threat continue unabated under President Obama? More importantly, does North Korea interpret it thusly? I submit that the deterrence of state sponsorship of nuclear terrorism falls somewhere in between “immediate” and “general” deterrence.⁹⁴ The situation cannot be described as a crisis, per se, though neither does it reflect the “relaxed,” regulated relationship of general deterrence.⁹⁵ As such, subsequent administrations must carefully consider how often, and how necessary it is, to reiterate the previously stated posture. In such an environment, the commitment of a new administration cannot be left as an assumption in the mind of an adversary.

Although questions of the character, or reputation, of the actor making deterrent threats also can affect credibility, I will address these in the “How Convincing?” section of this chapter. I now turn to the important question of exactly what action the United States should attempt to prevent.

B. PRECISELY WHAT ACTION?

A logical and useful foundation when formulating or analyzing any deterrence strategy is to determine precisely which undesired action or actions one wishes to prevent.⁹⁶ In our case, that action is state transfer of nuclear weapons or materials to terrorists. As it now stands, the U.S. threat implies the *purposeful* transfer of weapons and materials.⁹⁷ Several authors call for an expansion of this deterrence to include *unintentional* transfers to terrorists.⁹⁸ This is obviously a major distinction and carries

⁹⁴ Lawrence Freedman, *Deterrence* (Malden, MA: Polity Press), 2004, 40–42.

⁹⁵ Ibid.

⁹⁶ Jeffrey W. Knopf, “The Fourth Wave in Deterrence Research,” (unpublished manuscript, Naval Postgraduate School, June 2009), 47.

⁹⁷ I here assume a purposeful transfer includes only those transfers that are made as a result of strategic decisions by state leaders at the highest levels, thereby categorizing the actions of rebellious generals or scientists as unintentional from the reference point of the state. In the “Whom” section of this chapter, I analyze different referent objects of deterrence, to include purposeful transfer by individuals.

⁹⁸ Anders Corr, “Deterrence of Nuclear Terror: A Negligence Doctrine,” *The Nonproliferation Review* 12, no. 1 (2005): 127–147; Robert L. Gallucci, “Averting Nuclear Catastrophe,” *Harvard International Review* 26, no. 4 (2005); Elbridge A. Colby, “Expanded Deterrence: Broadening the Threat of Retaliation,” *Policy Review* no. 149 (June/July 2008): 43–59; Graham Allison, “The Only Thing that can Keep Nuclear Bombs Out of the Hands of Terrorists is a Brand-New Science of Nuclear Forensics,” *Newsweek* 153, no. 12 (March 23, 2009).

with it important implications. As Jeffrey Knopf points out, “it is inherently more plausible to deter some actions than others.”⁹⁹ I now analyze some of these proposals in order to determine the most appropriate target action for U.S. deterrence strategy in light of overall objectives and potential inherent tradeoffs.

Anders Corr recommends a policy of deterring both the intentional and accidental transfer of weapons or fissile material to terrorists.¹⁰⁰ He defines his “negligence doctrine” as the employment of policies designed to hold a state culpably negligent for “noncompliance with IAEA standards in the storage of fissile material [resulting] in that fissile material being lost or stolen and used for nuclear terror.”¹⁰¹ He includes in such policies the issuance of explicit deterrent threats, to include a proportional nuclear response, arguing that only these policies will provide the necessary incentive for certain states to sufficiently protect their fissile materials and nuclear weapons.¹⁰² He claims that cooperative programs not only have yielded less-than-stellar results to date, but they also create perverse incentives to “export” security at a steep price.¹⁰³ The solution, in his view, is to create incentives to better cooperation via deterrent threats.

Philipp Bleek finds that such policies, which he deems “deterrence of negligence,” would not significantly decrease the risk of nuclear terrorism and in many aspects may even intensify it.¹⁰⁴ He focuses specifically on the cases of Russia and Pakistan in arguing that an explicit deterrence-of-negligence policy would negatively affect existing cooperative programs by provoking these countries to be less transparent than they already are.¹⁰⁵ He acknowledges that, especially in the Russian case, perverse economic incentives may be hindering less than stellar cooperation and effort; however,

⁹⁹ Knopf, “The Fourth Wave in Deterrence Research,” 47.

¹⁰⁰ Corr, “Deterrence of Nuclear Terror: A Negligence Doctrine.”

¹⁰¹ Ibid., 133.

¹⁰² Ibid., 133–135.

¹⁰³ Ibid., 127.

¹⁰⁴ Phillip C. Bleek, “Would ‘Deterrence of Negligence’ Reduce the Risk of Catastrophic Terrorism?” (Draft 1.7.) Paper prepared for the 2006 Annual Meeting of the American Political Science Association, Philadelphia, PA, August 30–September 3, 2006.

¹⁰⁵ Ibid., 18.

he also points out that, negative incentives notwithstanding, Russia on its own is likely not capable of achieving the desired level of security.¹⁰⁶ Thus increased cooperation is necessary—the type of cooperation not typically achieved by resorting to overt threats.¹⁰⁷ Since a large degree of transparency and cooperation is likely necessary for a legitimate attribution result, and states fearing a painful retaliatory response for their unintentional negligence would be less inclined to cooperate both before and after a nuclear terrorist attack, Bleek suggests that such a policy would hinder efforts at preventing both initial and subsequent attacks.¹⁰⁸ In making these arguments, Bleek assumes deterrence-of-negligence threats are plausible, acknowledging that, if not, the debate is moot.¹⁰⁹

While not pausing for a thorough treatment of the plausibility of deterrence of negligence, I here infer the increased difficulty involved by pointing out that such a strategy more closely resembles compellence.¹¹⁰ Logically, a state cannot decide to unintentionally transfer weapons or materials to terrorists. Therefore, rather than deterring an unintentional action, deterrence of negligence actually intends to compel deliberate actions which, in turn, prevent the ultimately undesired action from transpiring accidentally. In such a compellence stance, the proverbial “Sword of Damocles” is hung above another state’s head, not to be dropped if the state initiates an action but if its failure to initiate certain actions—e.g., taking full and appropriate steps to secure fissile material stockpiles—results in an act of nuclear terrorism. It is inherently more difficult to achieve policy goals through compellence versus deterrence.¹¹¹

The above analysis indicates that the United States should primarily aim to deter the purposeful, vis-à-vis unintentional, transfer of nuclear weapons or materials to terrorist groups. This more plausible approach avoids provoking less cooperative

¹⁰⁶ Bleek, “Would ‘Deterrence of Negligence’ Reduce the Risk of Catastrophic Terrorism?” 20.

¹⁰⁷ Ibid.; see also Carter, et al., *The Day After: Action in the 24 Hours Following a Nuclear Blast in an American City*, 16.

¹⁰⁸ Ibid., 18–22.

¹⁰⁹ Ibid., 22.

¹¹⁰ Knopf, “The Fourth Wave in Deterrence Research,” 37.

¹¹¹ Freedman, *Deterrence*, 110; see also Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 70–86, for a thorough discussion of both the difference between deterrence and compellence, as well as additional difficulties inherent to compellence.

attitudes and actions from key international partners. This recommendation is not intended to preclude consideration, on a case-by-case basis, of announcing a deterrence-of-negligence position; however, much care must be taken to clearly communicate expectations, timelines, and methods for verification, with the ultimate goal of establishing a cooperative vice coercive regime.

Jeffrey Knopf describes a framework within which to consider the application of deterrence, with the broadest extreme labeled “systemic deterrence,” and the narrowest—“tailored deterrence.”¹¹² He advocates finding a middle ground between the two, the employment of which would include delineating a line that cannot be crossed, as well as describing situation- and actor-specific responses.¹¹³ In this case, the inviolable line should be the purposeful transfer of nuclear weapons or materials. This line might occasionally be shifted to include unintentional transfer in specific situations and for certain actors, but the shift must be communicated such that intentions and consequences are clearly understood by all actors. In the next section, I explore the sometimes complex relationship between the undesired actions and the actors to be deterred.

C. WHOM?

The behavior that the United States wishes to deter, at its simplest, is state transfer of nuclear weapons or materials to terrorists. Hence, the referent object of deterrence would appear to be the state. However, once the concept of the state is un-anthropomorphized, the problem becomes quite a bit more complex. The abstract concept of the “state” cannot transfer anything to anyone, per se. For purposeful transfer to terrorists to take place, any person or group of people who exercise control, however absolute or limited, over state nuclear assets would have to decide to effect such a transfer and then subsequently execute the decision. This list of people might include dictators, elected leaders, ruling councils, military leaders, and state nuclear scientists, among others. Must all of these actors be analyzed as potential targets for deterrence?

¹¹² Jeffrey W. Knopf, “Wrestling with Deterrence: Bush Administration Strategy after 9/11,” *Contemporary Security Policy* 29, no. 2 (2008): 230.

¹¹³ *Ibid.*

Proponents of the unitary-rational-actor approach might argue that the strategic significance of nuclear weapons and related technology dictates that a state maintain tight control over these assets. The head of state along with, possibly, a close circle of powerful elites, would exercise infallible decision-making authority. The state could thus be considered to act in a unitary, rational manner. In the case of Pakistani scientist A.Q. Khan and his proliferation network, however, significant divergence between the official government position and the actual administration of nuclear technology and secrets was evident.¹¹⁴ Though the buyers in Khan's network were not terrorists, it is not overly difficult to imagine terrorist buyers at the end of such a supply chain in the future. A deterrent posture based on a unitary-rational-actor model, possibly threatening massive retaliation for state transfer of nuclear assets, would likely not be effective in preventing such activity.

Alexander George is a proponent of an actor-specific approach.¹¹⁵ He suggests replacing the often-faulty assumptions made by the unitary-rational-actor model with all available information about an adversary's mindset, methods of calculating costs and risks, and the internal decision-making apparatus.¹¹⁶ This approach also takes into account asymmetric motivations and internally divergent interests.¹¹⁷ George takes care to distinguish between these conceptual models and the strategies based on them: "Concepts do not tell us what must be done in various situations with regard to specific adversaries in order to achieve deterrence."¹¹⁸ Strategies, however, are derived from these theoretical concepts and built to fit the context-dependent situation.¹¹⁹

¹¹⁴ International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, AQ Khan and the Rise of Proliferation Networks* (London: IISS, 2007), 65–67.

¹¹⁵ Alexander L. George, "The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries," *Comparative Strategy* 22, no. 5 (2003): 478–479.

¹¹⁶ *Ibid.*

¹¹⁷ *Ibid.*, 480.

¹¹⁸ George, "The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries," 480.

¹¹⁹ *Ibid.*

Although building detailed actor-specific conceptual decision-making models for each potential nuclear-terrorism sponsor is outside the scope of this thesis, it is still possible to make initial and general deterrence strategy recommendations based upon the apparent potential intent of each state. I now transition to a more practical analysis of potential deterrent targets, leaving to policymakers and analysts the detailed modeling and strategy construction best realized at classified information levels.

There are presently very few states in the world that would plausibly execute a purposeful transfer of nuclear weapons or materials to terrorists. North Korea, an international pariah likely possessing nuclear weapons and unknown quantities of HEU and plutonium, immediately comes to mind. Iran, currently enriching uranium though not yet believed to have a nuclear weapon, has a history of terrorist sponsorship as well as belligerence toward the West. Other states, such as Pakistan and Russia, are not presently threats with regard to purposeful transfer. Currently, the only two state targets for deterrence of purposeful transfer are North Korea and Iran.

On the other hand, a deterrence-of-negligence strategy could be applied to any state possessing nuclear fissile materials deemed not to meet protection and safeguard standards. As of 2005, 74 states together possessed over 3,700 tons of either HEU or plutonium.¹²⁰ Many of these states are developed countries and close allies of the United States.¹²¹ In contrast to former Soviet states, the United States does not provide financial assistance for nuclear security to developed states.¹²² However, diplomatic pressure has been successful at improving certain of these states' security measures in the past, and the relationships can generally be thought of as cooperative.¹²³ Applying a deterrence-of-negligence strategy to these states would be awkward at best, and counterproductive in the worst case.

¹²⁰ Institute for Science and International Security, "Global Stocks of Nuclear Explosive Materials: Summary Tables and Charts," ISIS Web site, http://isis-online.org/global_stocks/end2003/summary_global_stocks.pdf.

¹²¹ Bunn, *Securing the Bomb 2008*, 41.

¹²² *Ibid.*, 42.

¹²³ *Ibid.*

If deterrence-of-negligence threats would actually hinder the cooperation so essential to forensics-based attribution, then in cases where the potential for cooperation or some level of cooperation already exists, deterrence-of-negligence should not be chosen as a strategy. What, then, can be done to mitigate the possibility that a rebellious general or scientist may purposefully transfer materials to terrorists?

Although purposeful transfers by individuals are already addressed, in part, by cooperation regimes, stronger targeted deterrence strategies would help further reduce the risk. For example, various initiatives resulting from the 1991 Nunn-Lugar Act have helped to reemploy thousands of former Soviet weapons scientists in peaceful high-tech endeavors.¹²⁴ To further reduce the risk, individual actors might also be deterred by more severe threats of punishment.¹²⁵ Such a policy would fall under Knopf's framework as outlined above with the inviolable line set at purposeful transfer, and actor-specific responses outlined as necessary. For cases of sub-state individual or group actors some creative diplomacy might be required; for example, the purposeful transfer of nuclear materials or weapons to terrorists could be deemed a "crime against humanity," with justice to be meted out by the International Criminal Court. Short of that, the United States could work with individual countries to ensure citizens found guilty of violating this norm would be subject to the harshest of penalties. These cooperative and deterrence strategies would complement each other in states that are willing to cooperate. States that will not cooperate with the international community to reduce the risk of purposeful individual or overall unintentional transfer constitute a different case entirely.

Conveniently, the states that are the least likely to participate in cooperative regimes are also those most likely to purposefully transfer nuclear materials to terrorists. I now turn my attention back to North Korea and Iran. The need for deterrence to preclude purposeful transfer has been demonstrated; additionally, in these situations it is also essential to move the inviolable line to also cover unintentional transfer. This

¹²⁴ Richard G. Lugar, "The Nunn-Lugar Cooperative Threat Reduction Program," Official U.S. Senate Website of Senator Richard G. Lugar, <http://lugar.senate.gov/nunnlugar/>.

¹²⁵ Paul K. Davis and Brian M. Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda* (Santa Monica, CA: RAND Corporation, 2002), 40; Talmadge, "Deterring a Nuclear 9/11," 24–25; Colby, "Expanded Deterrence: Broadening the Threat of Retaliation," 45–50.

precludes these uncooperative regimes from claiming, after an attack and in order to avoid retribution, that the material was stolen or leaked by a lower-level operative.¹²⁶ Pre-attack deterrent threats also serve as a warning to these states that to possess nuclear weapons and materials brings with it a heavy and potentially consequential responsibility.

Summarizing my position on the referent objects of deterrence, I suggest that the U.S. government should treat non-cooperative, adversarial states as unitary, though not necessarily rational, actors. Conversely, the United States must look inside cooperative, friendly states to find specific objects for deterrence. Actor-specific analyses can and should be utilized in both cases. For both types of states the expectation must be that the tightest of control is exerted over nuclear weapons and materials; however, this problem cannot be assumed away. It is best addressed with a mixture of cooperative and individual-actor-specific deterrence strategies in friendly states, and with a unitary-actor deterrence strategy when dealing with adversarial states.

Now that I have addressed both what the United States should reasonably attempt to deter and the list of adversaries that should be targets of this deterrence, I turn to the last element of the deterrence construct.

D. HOW CONVINCING?

In this section, I analyze deterrence strategy in light of theoretical propositions for deterrence success and failure. Richard Ned Lebow identifies four primary conditions for successful deterrence: a clearly defined commitment, the effective communication of the commitment to adversaries, the capability to act in defense of the commitment, and a demonstration of the resolve, or intent, to carry out the threatened actions.¹²⁷ These factors together constitute the basis for the credibility of a given deterrent stance. Lebow is careful to point out, however, that credibility ultimately is a subjective concept that resides in the mind of the adversary.¹²⁸ As such, it is extremely difficult to measure and

¹²⁶ Michael A. Levi, *Deterring State Sponsorship of Nuclear Terrorism* (New York, NY: Council on Foreign Relations, 2008), 20.

¹²⁷ Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981), 84–85.

¹²⁸ *Ibid.*, 83–84.

assess.¹²⁹ Lebow suggests that his primary conditions may be used to gauge the credibility of a given deterrence strategy. This is the technique I here apply to current and potential U.S. deterrence strategy regarding state support for nuclear terrorism.

1. Commitment—Clearly Defined and Communicated

The commitment of the United States to protect its citizens and homeland, especially from the horror of nuclear terrorism, is obviously strong and should be implicitly understood. This basic commitment should never be a question in the mind of any possible state sponsor of terrorism. The commitment to prevent the transfer of nuclear weapons or materials to terrorists, directly enabling an attack on the United States, could be seen as nearly equally strong, but this cannot be left implicit. Since the act of transferring weapons or materials to terrorists enables an attack, but in itself is not the attack, the United States must clearly communicate its intent to treat those who enable an attack equally as culpable as those who execute the attack.

The United States has indeed made this clear in the most general sense.¹³⁰ What remains is for the nation to determine in what cases it will treat the unintentional transfer as the equivalent of intentional, how explicitly it should communicate such nuances to adversaries, and how explicitly and specifically it should communicate deterrent threats.

2. Capability

According to Lebow, the defensibility of a commitment can be thought of in terms of either actual military defense or the ability to retaliate against the adversary.¹³¹ The United States possesses more than adequate military capability to respond to adversaries that sponsor nuclear terrorism. The crux of the capability problem, however, lies not in military capability to respond, but in the U.S. government's capability to

¹²⁹ Lebow, *Between Peace and War: The Nature of International Crisis*, 83–84.

¹³⁰ See official strategy as outlined in Office of the President, *National Strategy for Combating Terrorism*, 14–15, reference to then-President Bush's deterrence declaration in Phillips, "Uncertain Justice for Nuclear Terror," 441, and an analysis of a speech by then-National Security Advisor Stephen Hadley in Colby, "The New Deterrence" for a picture of U.S. intent as publicly declared.

¹³¹ Lebow, *Between Peace and War: The Nature of International Crisis*, 88.

reliably attribute state sponsorship of a nuclear attack. This begs the question: how does an imperfect attribution capability affect the credibility of U.S. deterrent threats? Additionally, should the United States modify its threats based upon the current inexact nature of the art and science of attribution?

Michael Levi tackles these problems in some depth. Correctly maintaining that nuclear forensics-based attribution will never achieve perfection, he nonetheless uses the assumption of perfection in establishing a preferred-policy baseline before assessing the impact of an imperfect capability.¹³² To get around the problem of an imperfect attribution capability, Levi recommends “split[ting] the burden of proof,” such that retaliation would be based upon strong but not infallible evidence.¹³³ This would ostensibly force a state accused on the basis of such strong evidence to demonstrate that it was not, in fact, involved. The state would need to make all aspects of its nuclear programs and materials transparent and available, which would be very difficult practically to accomplish with a sufficient degree of trust. This difficulty, coupled with the knowledge that retaliation could come as a result of strong evidence, should serve to make the deterrent threat more credible in the mind of an adversary.

Therefore, with the adoption of a deterrence strategy based upon a split burden of proof, the capability aspect of deterrence credibility should not suffer as long as the attribution capability of the United States is sufficient to gather compelling evidence. Levi asserts that U.S. ability to create a robust attribution case would be strong regarding North Korea and relatively weak for Russia, Pakistan, and Iran; he bases this assertion on the accessibility of nuclear material databases for each state in question.¹³⁴ This provides additional support for treating North Korea as a special case. However, even in a situation where U.S. capability is plausible, it is important to ask how an attribution case resting on imperfect evidence would affect U.S. intent to respond. I address this and other issues of intent in the following paragraphs.

¹³² Levi, *Deterring State Sponsorship of Nuclear Terrorism*, 17–19.

¹³³ Ibid.

¹³⁴ Ibid., 18–24.

3. Intent

The United States' intent to respond may be questioned based on the strength of evidence supporting an attribution claim, on the nature of the deterrent threat itself, and on reputational factors. I first focus on how an imperfect attribution capability might affect the U.S. intent to respond, linking that intention to the explicit pre-attack threat, before transitioning to a discussion of reputational factors.

Clearly, the United States would intend to respond based upon absolute proof of state complicity in a nuclear attack. Would an adversary perceive the same intent if U.S. retaliatory policy was based upon strong evidence alone? I submit that it would depend on the nature of the threatened response. There are moral problems inherent in any military retaliation visited upon a state that may be innocent, however small that possibility may be.¹³⁵ These moral problems increase, and credibility proportionately decreases, with each degree of violence explicit in the threatened response. Although, to the degree that innocents would suffer for the actions of a few, it might be argued that this graduated moral dilemma would exist even with perfect attribution confidence, I contend that the effect is magnified when retaliatory threats are based on imperfect evidence. The choice of threatened response is critical, then, as it cannot be so extreme as to strain credibility yet must threaten pain sufficient to deter.

Regardless of attribution confidence, an explicit threat to retaliate with nuclear weapons would likely not be perceived as credible. Richard Price and Nina Tannenwald find that the non-use of nuclear weapons after 1945 can be accounted for not by rational deterrence alone, but with a normative element as well.¹³⁶ Lawrence Freedman points out that, whether nuclear use is inhibited by normative pressure or simply by fear of retaliation in kind, there is a large political cost inherent in the use of nuclear weapons.¹³⁷

¹³⁵ Levi takes a slightly different view, limiting such moral constraints to the use of nuclear weapons, the targeting of civilians, and considerations of potential counter-retaliation against U.S. allies. See Levi, *Detering State Sponsorship of Nuclear Terrorism*, 18, and related footnote (19).

¹³⁶ Richard Price and Nina Tannenwald, "Norms and Deterrence: The Nuclear and Chemical Weapons Taboos," in *The Culture of National Security: Norms and Identity in World Politics*, ed. Peter J. Katzenstein (New York: Columbia University Press, 1996), 114.

¹³⁷ Freedman, *Deterrence*, 69–71.

Indeed, both rational deterrence and norms help to explain the implausibility of a nuclear response.¹³⁸ From a rational perspective, a target state armed with even a small number of nuclear weapons would have deterrent leverage in the form of a potential counter-retaliation strike. A U.S. nuclear retaliatory first-strike intended to destroy the target state's capacity for counter-retaliation, in the process killing many thousands of citizens, would be beyond all moral justification and egregiously violate the established norm of nuclear non-use.

The threat of regime-change via conventional military attack is much more plausible from a normative perspective, though attacking a nuclear-armed state, even with conventional weapons, is similarly problematic to the situation described immediately above. Such a strategy would have to be carefully executed to avoid placing the targeted state's leadership in a situation where they feel they have nothing to lose. Would a less severe threat then be in order?

Any explicit pre-attack threat less severe than regime change would be unpalatable for a number of reasons. First, the possibility that a regime, which sponsored a terrorist nuclear attack against the United States, could remain in power would not be well-received by the American people. Second, it would be difficult to find a target set that could approach the equivalent pain level of a nuclear attack in a U.S. city. Third, threatening anything short of regime change might not increase the calculated cost sufficiently to affect deterrence in the mind of the adversary.

This dilemma is best solved by distinguishing between pre-attack threats and actual post-attack response. A purposefully ambiguous pre-attack threat to respond severely would credibly convey to an adversary that there would be a high cost to pay; it would also leave all post-attack response options open.¹³⁹ I make recommendations regarding each component of strategy later in this chapter. I now turn to reputational factors of credibility.

¹³⁸ Freedman, *Deterrence*, 71.

¹³⁹ Phillips, "Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution," 442.

Although the effect of reputational factors on credibility is debatable, I argue that the United States is well positioned regardless. Lawrence Freedman reviews arguments for and against the importance of reputation before concluding that, “assumptions will have to be made about character, and these must come from somewhere ... there is no reason to suppose that past impressions are irrelevant.”¹⁴⁰ Daryl Press sets out to demonstrate that a state’s credibility is not determined by its past behavior, but rather the present calculation of capabilities and interests involved.¹⁴¹ If, indeed, reputation based on past behavior is an important variable influencing credibility, the United States has made a strong case for resolute response with its actions in both Afghanistan and Iraq. If the opposite is true and the present balance of capabilities and interests trumps reputation as an influential variable, again the United States has a strong case in that a nuclear attack on its homeland is undoubtedly an attack on a vital interest.

Interestingly, Press demonstrates that concerns for future credibility often spur leaders to pursue aggressive foreign-policy options.¹⁴² Such concerns, indeed, may enter into decision makers’ thinking after a terrorist nuclear attack, leading them to elect an extreme response. This may be mitigated, in part, by the length of time required for attribution analysis and the adversarial process inherent in the democratic system. Regardless of the effect of this phenomenon, it should not prove detrimental to the credibility of U.S. pre-attack deterrent posture.

I have now completed an analysis of the deterrence concept with regard to deterrence of state sponsorship of nuclear terrorism, analyzing *who* is deterring *whom* from initiating *precisely what action*, and *how* this *convincing* takes place, applying various deterrence theories to practice. Before making recommendations based upon this application of theory to strategy, I briefly address an additional reason for deterrence failure.

¹⁴⁰ Freedman, *Deterrence*, 53–56.

¹⁴¹ Daryl G. Press, *Calculating Credibility: How Leaders Assess Military Threats* (Ithaca, NY: Cornell University Press, 2005), 20–21.

¹⁴² Press, *Calculating Credibility: How Leaders Assess Military Threats*, 12–13.

E. DETERRENCE FAILURE

Deterrence can fail for any number of reasons, some of which were either directly addressed or at least alluded to above. These include, among others, an incredible deterrent threat, an insufficient communication or signaling of intent, and a miscalculation of gains and losses. I here wish to address an additional reason for deterrence failure that was not obvious from the above discussion.

Jeffrey Berejikian presents a theory of deterrence based not on traditional rational choice, but on certain cognitive assumptions that fall under the label of “prospect theory.”¹⁴³ He finds that “decisionmakers do not maximize in their choices, are apt to overweight losses with respect to comparable gains and tend to be risk averse when confronted with choices between gains while risk acceptant when confronted with losses.”¹⁴⁴ These choices are made relative to a reference point, which is often the status quo. A state that perceives the status quo as satisfactory or beneficial is operating in a “gains frame;” conversely, a state dissatisfied with the status quo is operating under a “losses frame.”¹⁴⁵ Deterrence can fail when a state is already in or is forced into a losses frame.¹⁴⁶ In fact, Berejikian warns that the deterrent threat itself may push a state into a losses frame.¹⁴⁷ His hypothesis holds interesting implications for both North Korea and Iran.

North Korea has been expressing dissatisfaction with the status quo for some time, while Iran’s situation is more difficult to discern. Given the inherently low attractiveness of sponsoring nuclear terrorism,¹⁴⁸ a state reasonably satisfied with the

¹⁴³ Jeffrey D. Berejikian, “A Cognitive Theory of Deterrence,” *Journal of Peace Research* 39, no. 2 (2002): 165.

¹⁴⁴ Ibid.

¹⁴⁵ Ibid., 173.

¹⁴⁶ Ibid., 176–178.

¹⁴⁷ Ibid., 179.

¹⁴⁸ Knopf, “The Fourth Wave in Deterrence Research,” 35–36. Knopf suggests that, apart from hatred and a desire to punish, the enabling of a terrorist nuclear attack on the United States would fail to achieve any plausible policy objective of a rogue state.

status quo should be readily deterred, even by an imperfectly credible deterrent threat.¹⁴⁹ However, if North Korea or Iran were operating in a losses frame, one of them might consider sponsoring nuclear terrorism, perhaps reasoning there was little to lose.¹⁵⁰ This calculation, of course, depends upon the extent of despair. Tools of coercive diplomacy such as international pressure and economic sanctions, for all of their potential benefits, more likely than not force these states further into a losses frame.¹⁵¹ Adversary perceptions of the status quo, therefore, are important. The United States must be cognizant of the ways in which its foreign policy affects these perceptions.

The United States' use of the so-called "Bush Doctrine" of preemption in effecting regime change in Iraq, coupled with the labeling of both North Korea and Iran as part of the "axis of evil," serves to implicitly threaten both of those states as well.¹⁵² Both North Korea and Iran, then, may rightfully equate the status quo with the open-ended threat of regime change. If this threat exists regardless of their actions regarding sponsorship of nuclear terrorism, any related deterrence strategy based upon a threat of regime change—and thus by definition not increasing their cost over the status quo—would be entirely ineffective.¹⁵³ To be fair, this status-quo threat of regime change has been attenuated to a certain degree by the change of U.S. presidential administrations, the length and expense of the U.S. efforts in Iraq and Afghanistan, and President Obama's "outstretched hand" engagement policy. Nevertheless, more explicit assurances need to be given such that both states understand their security depends on their own actions and not on U.S. policy whims.

¹⁴⁹ Berejikian, "A Cognitive Theory of Deterrence," 175.

¹⁵⁰ S. Paul Kapur, "Deterring Nuclear Terrorists," in *Complex Deterrence: Strategy in the Golden Age*, ed. T. V. Paul, Patrick M. Morgan, and James J. Wirtz (Chicago: University of Chicago Press, 2009), 113. Kapur proposes that financial desperation might entice North Korea to risk selling fissile material to the highest bidder on the black market.

¹⁵¹ Berejikian, "A Cognitive Theory of Deterrence," 179.

¹⁵² Knopf, "Deterrence or Preemption," 396.

¹⁵³ *Ibid.*, 396. Knopf highlights the critical importance of pairing assurances with deterrence.

F. IMPLICATIONS AND POLICY RECOMMENDATIONS

I now point out several policy implications and make some recommendations on the basis of the above discussion. These involve the focus of U.S. deterrence strategy, the nature of pre-attack deterrent threats as well as post-attack retaliatory actions, and status-quo actions and programs that must be changed, continued, or further developed.

Since a deterrence-of-negligence policy would not result in the desired degree of international cooperation, the United States can significantly narrow the focus of its deterrent posture with regard to state sponsorship of nuclear terrorism. Only antagonistic nuclear states should be targeted. This narrow focus, then, utilizes a forensics-based attribution capability as a precise instrument for deterrence purposes, enabling the crafting of actor-specific deterrence policies for these few existing (and future) legitimate deterrence targets. I reserve a more detailed discussion of legitimate deterrent targets and appropriate deterrent threats for Chapter V. I now address strategic recommendations for response in the event of deterrence failure.

If the unthinkable were to happen, how should the United States respond? For the sake of argument, let us assume that after a terrorist nuclear attack the United States finds compelling—but not 100% conclusive—evidence that North Korea was the source of the fissile materials used to construct the bomb. Given the current limitations of nuclear forensics-based attribution science, this is not an unlikely scenario. The best way forward requires carefully balancing at least two important concerns.

A first priority after a nuclear terrorist strike would be the prevention of another. Levi correctly asserts that a large degree of international cooperation, even with the offending state sponsor, would be required to gather and act upon all available and necessary information.¹⁵⁴ He recommends a retaliatory policy that is “strong enough to maintain U.S. credibility but that is restrained enough to leave open the possibility of additional action if North Korean leaders do not cooperate in preventing further

¹⁵⁴ Knopf, “Deterrence or Preemption,” 21–26.

attacks.”¹⁵⁵ Such an approach would be difficult to find in practice—what, after all, would be strong enough to maintain U.S. credibility after absorbing a nuclear attack short of nuclear retaliation or regime change?

This leads to the second major concern in responding to North Korea after a terrorist nuclear attack—any attack on a nuclear-armed state must obviously be approached very cautiously. North Korea might attempt to deter a U.S. retaliatory attack by threatening a nuclear or conventional counter-retaliation on South Korea or Japan.

I propose that both of these dilemmas could be mitigated by first issuing an ultimatum demanding North Korea’s submission to nuclear disarmament.¹⁵⁶ As part of this ultimatum, an international regime would be established to verify and monitor disarmament. North Korea would relinquish any right to the peaceful use of nuclear technology, and a continuous monitoring presence would be established to ensure compliance. Assurances might have to be given such that compliance would avoid further violence. This would, regrettably, keep the offending regime in power, yet would also offer a solution to the problem of needing the offender’s help in preventing follow-on attacks.¹⁵⁷ The United States might also demand that North Korea turn over for prosecution those individuals responsible for making and executing the decision to sponsor nuclear terrorism. Rejection of these ultimatums would give the United States sufficient cause, as well as moral justification, to proceed with forcible disarmament and regime change, using “overwhelming force” if necessary.¹⁵⁸

I have just addressed what I see as the best option for post-attack response. In a more perfect world, of course, deterrence would not fail. Toward that end, I now recommend some actions the United States should take to improve the status quo in order to complement and bolster its deterrent efforts.

¹⁵⁵ Knopf, “Deterrence or Preemption,” 17.

¹⁵⁶ Phillips, “Uncertain Justice for Nuclear Terror,” 436. Phillips lists disarmament as one of several possible demands that could be made of suspect states after the “transformative event” of a terrorist nuclear attack when attribution results are inconclusive.

¹⁵⁷ Levi, *Deterring State Sponsorship of Nuclear Terrorism*, 21–26.

¹⁵⁸ This would have to undertaken with extreme care, especially in the case of a nuclear-armed adversary, such as North Korea. Any adversary threats or actions to launch nuclear strikes on allies of the United States could be met with intense and even “overwhelming” efforts to eliminate this possibility.

The United States must continue to develop its forensics-based attribution capability, both generally and specifically with regard to North Korea and Iran. Although perfection is almost certainly unattainable, continuous improvement is necessary. Program successes should be widely advertised in order to give the U.S. deterrent threat more probabilistic credibility.¹⁵⁹ Every degree of certainty with which a post-attack attribution claim can be made increases response options and lessens the inherent moral baggage involved.

The United States must continue to emphasize cooperative programs to secure fissile materials around the world. Since compellence strategies are less effective in this area, much more political emphasis must be placed on cooperation in its various forms. More political capital must be spent by the President and other top American diplomats.

The United States must be aware, particularly with regard to North Korea and Iran, that its policies can work to increase or decrease those states' satisfaction with the status quo. This has important ramifications for deterrence success, as discussed above. This is not to say that the United States needs to actively work to make the world a better place for "rogue" regimes, only that there is a point at which certain coercive pressures can make risky status-quo altering options more appealing to adversaries.

G. CHAPTER SUMMARY

The art and science of forensics-based attack attribution enables a deterrent posture that fills a critical strategy gap in the prevention of nuclear terrorism. Deterrence theory supports the belief that attribution capability need not be infallible to offer a credible pre-attack deterrent posture, though the strength of any post-attack attribution claim will directly affect the range of possible responses. With this in mind, the United States is best served by explicitly targeting the states and actions it wishes to deter while leaving the deterrent threats ambiguous. This ambiguity leaves open the widest range of retaliatory options in the event of deterrence failure leading to attack, options that would have to be pursued cautiously in light of multiple post-attack variables in an extremely

¹⁵⁹ Talmadge, "Deterring a Nuclear 9/11," 29–32; Ferguson, "Can Nuclear Forensics Trace a Detonated Nuclear Weapon to its Source?" 7–8.

challenging environment of intense domestic and international pressures. This exploration of deterrence theory and U.S. strategic and policy goals has indicated the wisdom of limiting the application of attribution-enabled deterrence to adversarial states, while insisting on the furtherance of cooperative regimes with all other states. The United States needs to make some adjustments to its stated deterrent posture with regard to state sponsorship of nuclear terrorism, while maximizing efforts to improve both its attribution capability, as well as international cooperative regimes.

IV. POST-DETONATION ATTRIBUTION CAPABILITY

In this chapter, I examine the role of post-detonation nuclear forensics in the attribution of responsibility for the provision of nuclear materials used in a terrorist nuclear attack on the U.S. Homeland. I will examine the levels of reliability and accuracy with regard to forensic technology and support required for a sufficient attribution capability, addressing current critical gaps. If the United States does not currently possess these levels of reliability and accuracy, are they achievable in the near term and at a cost it can afford to pay?

I begin the exploration with some necessary definitions along with an overview of the nuclear forensic process, to include a plausible timeline for expected results. From a review of the literature and case studies involving pre-detonation nuclear forensics, I make a qualitative overall assessment of the nation's current capabilities. I then break the entire nuclear forensic and attribution process into its various components, extracting from the literature some widely agreed-upon requirements for a sufficient attribution capability. Following the determination of requirements for each component, I analyze the current state of U.S. capability as well as identify critical gaps. I then provide a general assessment of the likely costs—fiscal, opportunity, and political-capital—needed to improve and sustain a credible attribution capability.

I find that although some aspects of the program are fairly well developed, in its current state the attribution program has not achieved the desired capacity. I am not confident that, were a nuclear attack to take place today in an American city, the government would be able to authoritatively trace the attack back to its state sponsor. Although attribution-program perfection will never be achieved, existing capability gaps can be closed to a sufficient degree to enable credible deterrence. The costs of closing these capability gaps, expensive primarily in terms of political capital, must be addressed with political focus over both the short and long term.

A. NUCLEAR FORENSICS—SOME DEFINITIONS

In their leading textbook on nuclear forensic science, Kenton Moody et al. define forensic science, in general, as: “the application of any appropriate technical or sociologic discipline to narrow the limits of informed conjecture.”¹⁶⁰ The limitations inherent in any type of forensic analysis should be evident from this definition—“the limits of ... conjecture” are narrowed, not eliminated altogether, and “informed conjecture” is still, after all, conjecture. Thus while nuclear forensic science provides a critical component of an overall attribution capability, it functions well only in concert with robust intelligence and law enforcement support, and does not offer in any case a guarantee of successful attribution.

A report by the Nuclear Forensics Working Group of the American Physical Society and the American Association for the Advancement of Science provides a more specific definition for nuclear forensics: “Nuclear forensics is the technical means by which nuclear materials, whether intercepted intact or retrieved from post-explosion debris, are characterized (as to composition, physical condition, age, provenance, history) and interpreted (as to provenance, industrial history, and implications for nuclear device design).”¹⁶¹ Although pre- and post-detonation nuclear forensic processes rest on the same scientific principles, I largely limit the focus of this chapter to post-detonation attribution. Post-detonation forensic analysis and attack attribution present more complex challenges for both investigators and policymakers.

B. NUCLEAR FORENSICS IN THE CONTEXT OF ATTACK ATTRIBUTION—THE PROCESS

Following a nuclear terrorist attack on a U.S. city, in addition to all considerations of initial response and recovery, authorities would be under enormous pressure to determine the source of the attack. Terrorists may claim to have one or more additional nuclear weapons at their disposal, with goals from extortion to provoking widespread

¹⁶⁰ Kenton J. Moody, Ian D. Hutcheon, and Patrick M. Grant, *Nuclear Forensic Analysis* (Boca Raton, FL: CRC Press, Taylor & Francis Group, 2005), vi.

¹⁶¹ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 3.

panic and disruption on an enormous scale.¹⁶² Regardless, it would be prudent for decision makers to assume that the group did, in fact, have additional weapons.¹⁶³ Decision makers would need to know which state, wittingly or not, facilitated the terrorists in procuring the bomb or the nuclear material necessary to construct it. This knowledge would focus intelligence-gathering and law-enforcement efforts, ultimately facilitating a realistic assessment of the likelihood of a follow-on attack, inhibiting further transfers, and informing retaliatory options. How, then, would this determination unfold? What steps are involved in the process of attributing responsibility?

The immediate and perhaps obvious task for investigators following any large detonation is to determine whether the blast was nuclear or not. Supporting evidence comes in many forms: Air Force “Defense Support Program” satellites equipped with infrared sensors designed to detect nuclear detonations,¹⁶⁴ seismic and noble gas sensors maintained by the Comprehensive Test Ban Treaty Organization’s Global Monitoring System,¹⁶⁵ radiation detection equipment maintained by various federal agencies, visual evidence as provided by a mushroom cloud, aerial or satellite photography conveying the magnitude of destruction, and a determination of the distance at which windows withstood the blast from the shock wave.¹⁶⁶ This nuclear determination and yield measurement becomes more difficult and time-consuming when dealing with sub-kiloton nuclear blasts.¹⁶⁷ Such preliminary indications of a nuclear detonation would set teams of experts and scientists across many departments and located around the nation in motion, some to gather evidence and some to prepare to receive, analyze, and begin to interpret the evidence.

¹⁶² Bunn, *The Risk of Nuclear Terrorism—And Next Steps to Reduce the Danger*, 5.

¹⁶³ Carter et al., *The Day After: Action in the 24 Hours Following a Nuclear Blast in an American City*, 14–15.

¹⁶⁴ Global Security, “Defense Support Program,” <http://www.globalsecurity.org/space/systems/dsp.htm>.

¹⁶⁵ Comprehensive Test Ban Treaty Organization, “Verification Regime: CTBTO Preparatory Commission,” <http://www.ctbto.org/verification-regime/>.

¹⁶⁶ William Dunlop and Harold Smith, “Who did it? Using International Forensics to Detect and Deter Nuclear Terrorism,” *Arms Control Today* 36, no. 8 (October 2006): 7.

¹⁶⁷ Michael May, Jay Davis, and Raymond Jeanloz, “Preparing for the Worst,” *Nature* 443, no. 7114 (October 26, 2006): 908.

Sufficient debris from a nuclear weapon can be collected even after a nuclear explosion. Since only a small percentage of the fissile material in a weapon actually undergoes fission, much of the other nuclear material is left behind, albeit in the form of tiny fragments spread over a large area.¹⁶⁸ Significant amounts of this material can be collected on the ground by robots or personnel with special equipment, and in the air by specially outfitted Air Force aircraft.¹⁶⁹ This debris, after retrieval, would then be transported to one or more national laboratories for forensic analysis.

Scientists have many analytical tools at their disposal in conducting nuclear forensic analysis of recovered materials. Elemental and isotopic bulk analysis tools include chemical assay, radiochemistry, radioactive counting techniques, and several methods of mass spectrometry.¹⁷⁰ Imaging tools, though less applicable for post- versus pre-detonation forensics, include visual inspection and photography as well as optical and electron microscopy. Microanalysis tools include X-ray microanalysis and infrared spectroscopy. The process of selecting appropriate methods is iterative, with the results of one test suggesting one or more specific follow-on tests.¹⁷¹ Additionally, certain tests are destructive in nature, making the “proper selection and sequencing of analyses ... critical.”¹⁷²

These tests will be able to determine several facts with a fairly high degree of certainty: 1) Whether the weapon was built using HEU or plutonium; 2) If the weapon used HEU, the degree of enrichment with uranium-235; 3) If the weapon used plutonium, various isotopic signatures (time the fuel was in a nuclear reactor, time since separated from spent fuel) indicative of the production process.¹⁷³ In turn, from such evidence the

¹⁶⁸ May et al., “Preparing for the Worst,” 907.

¹⁶⁹ William J. Broad, “Addressing the Unthinkable, U.S. Revives Study of Fallout,” *The New York Times*, March 19, 2004, <http://www.nytimes.com/2004/03/19/us/addressing-the-unthinkable-us-revives-study-of-fallout.html?scp=1&sq=Addressing%20the%20Unthinkable&st=cse&pagewanted=all>.

¹⁷⁰ See International Atomic Energy Agency, “Nuclear Forensics Support,” *IAEA Nuclear Security Series 2* (2006), 46–54, for a detailed description of each of the techniques enumerated in this paragraph.

¹⁷¹ See International Atomic Energy Agency, “Nuclear Forensics Support,” 24.

¹⁷² *Ibid.*

¹⁷³ Dunlop and Smith, “Who did it? Using International Forensics to Detect and Deter Nuclear Terrorism?” 7.

sophistication of the weapon or even a certain bomb design might be inferred.¹⁷⁴ An important distinction must here be emphasized: a thorough nuclear forensic analysis should establish various signatures for the material in question,¹⁷⁵ while such signatures may narrow the range of possible sources, a definite attribution cannot be made without matching the determined signatures to those associated with a known source.

At this point in the attribution process, scientists would attempt to match the various signatures determined via nuclear forensics with existing signatures stored in databases worldwide. Such source signatures can be either empirically derived from actual material samples or computer-generated, predictive signature models based upon the chemistry and physics behind nuclear processes.¹⁷⁶ Although predictive signatures have some value in the absence of empirical signatures, empirical signatures lend much greater clarity and credence to the attribution process.¹⁷⁷ As multiple signatures can be determined for any given sample, attribution is stronger when multiple signatures can be matched to known existing signatures. As more signatures become available during the forensic process, intelligence-gathering and law-enforcement efforts can be more narrowly focused; the results of such efforts should be used to strengthen or confirm the ultimate forensic attribution determination. How long is this entire process likely to take and what are the expected timelines for the various results?

Although no guaranteed timeline for forensic analysis results exists, several authors provide approximate overviews of the procedural timeline.¹⁷⁸ Many questions are asked throughout the attribution process, and the promptness of the answers often depends upon the physical limitations of nuclear science (e.g., determining a signature based on a decaying half-life takes a certain amount of time, by definition). Additionally,

¹⁷⁴ Dunlop and Smith, “Who did it? Using International Forensics to Detect and Deter Nuclear Terrorism?” 7.

¹⁷⁵ A signature is the distinguishing characteristic, or set of characteristics, that make a nuclear sample unique.

¹⁷⁶ See International Atomic Energy Agency, “Nuclear Forensics Support,” 32.

¹⁷⁷ *Ibid.*, 45. Also see 45–51 for a more in-depth, technical discussion of the relative importance of empirical over predictive signatures.

¹⁷⁸ See Michael Miller, “Nuclear Attribution as Deterrence,” *The Nonproliferation Review* 14, no. 1 (2007): 37–39 for the most thorough example of such a timeline.

the complexity of nuclear forensic science cannot be overstated. Its seminal textbook forthrightly states, “Radiochemical forensic analysis is a labor-intensive activity.”¹⁷⁹ Keeping these difficulties in mind, it is possible to frame windows of time during which specific questions could be answered and determinations made via nuclear forensics during the attribution process.

Were a nuclear detonation to occur in an American city, nuclear forensic teams should be able to determine within hours if the blast was truly nuclear in nature as well as to approximate the explosive yield.¹⁸⁰ Within a window of hours to days of the blast, experts would determine whether uranium or plutonium was used, as well as categorize the sophistication of the device itself. Several days after laboratory analysis began, scientists would know the isotopic compositions of the nuclear materials, and with that information begin to make inferences regarding the material’s history. Data from known nuclear weapons tests would be searched to look for possible similarities or matches. Several weeks after laboratory analysis began, scientists should be able to estimate the most probable weapon design, as well as search for similarities or matches with known existing designs.

The strength of any forensics-based attribution claim would depend on the strength of signature matches; absent a match with either an actual sample or data derived from an actual sample, a credible forensics-based claim in any length of time is unlikely.¹⁸¹ Throughout the course of this process, intelligence and law enforcement information might be used to provide the political impetus necessary to gather signature data and actual samples from sources theretofore unavailable. Likewise, information from the ongoing nuclear forensics analysis might serve to focus intelligence and law enforcement information-gathering efforts. Coupled with authoritative intelligence, even a forensics-based hypothesis based upon predictive signatures can become a credible basis for an attributive claim. In summary, then, scientists might have enough forensic

¹⁷⁹ Moody et al., *Nuclear Forensic Analysis*, 241.

¹⁸⁰ The timeline in this paragraph is derived from Joint Working Group, *Nuclear Forensics*, 5; May et al., “Preparing for the Worst,” 908; and Miller, “Nuclear Attribution as Deterrence,” 37–39.

¹⁸¹ Miller, “Nuclear Attribution as Deterrence,” 41.

information after just a few weeks to narrow the field of possible sources, perhaps even hypothesizing that a particular source is the likely candidate. However, absent a match with a known, existing signature from such a source, convincing attribution is not possible without additional and authoritative intelligence.

This primer has provided a basic overview of the process, to include the steps that would be taken after an attack to gather and analyze evidence. The capabilities and limitations of the scientific tests were emphasized, as was the importance of signature matching and the necessity of databases. This section concluded with a brief exposition of a possible timeline for expected results following a detonation. The question now becomes—how robust is the current U.S. attribution capability?

In answering that question, I begin with a general assessment of current U.S. capability as gleaned through a literature review of open-source material. I will then examine the following components of an attribution program in more detail: scientific limitations and requirements, nuclear materials database, intelligence support, law enforcement support, and exercise requirements. I have carefully selected these components for the major role each plays in an attribution capability. In progressing through each, I will describe the requirements necessary for a fully functioning, credible attribution program. From this examination, a picture of how far and in what ways the United States falls short should become clearer, as should the path toward achieving success. I conclude by briefly addressing some potential costs involved.

C. OVERALL CURRENT CAPABILITY ASSESSMENT

To date, terrorist nuclear attacks have remained in the realm of imagination. Novelists and screenwriters have capitalized on the threat to sell books and movies, and policymakers have long imagined the worst and worked to prevent it. The protagonist in Tom Clancy's *The Sum of All Fears* receives a source determination from a nuclear forensics team within minutes of its arrival on scene, assimilates that information with specific intelligence on the supply chain, and quickly determines the terrorist perpetrators

and their state sponsor.¹⁸² Fiction writers often take such overly optimistic license with reality; policy- and decision makers cannot afford to. What, then, should decision makers expect from the nation's current attribution capability?

Most scholars and other experts in the field make a less-than-optimistic characterization of the overall current capability to attribute a terrorist nuclear attack based upon nuclear forensics and support. Charles Ferguson highlights physicists' incomplete understanding of the fission process as it impacts forensic analysis, emphasizes the need for a significant expansion of sample databases, and points out the existence of methods for deceptively altering nuclear materials to conceal their source.¹⁸³ Caitlin Talmadge outlines technical, political, and diplomatic challenges to establishing credible deterrence through attribution before advocating an increased investment in forensic analysis technology.¹⁸⁴ Michael Miller provides a thorough treatment of "well developed but not foolproof" forensic technology.¹⁸⁵ Matthew Phillips focuses on the limits to forensic analysis as determined by the physical science itself, concluding pessimistically that even vast improvement in capabilities will not allow the guarantee of definitive attribution.¹⁸⁶

Since post-detonation nuclear forensics-based attribution will not truly be tested until the unthinkable happens, case studies are non-existent. Exercise results are understandably classified; regardless, exercises cannot nearly approach realistic simulation of post-attack conditions. However, case studies of pre-detonation forensics performed on surrendered or interdicted fissile materials provide implications that do, in fact, apply to both pre- and post-detonation attribution processes. Such cases also provide a qualitative feel for the current capabilities of national and international nuclear forensics in a pre- or post-detonation attribution process.

¹⁸² Miller, "Nuclear Attribution as Deterrence," 33–34.

¹⁸³ Ferguson, "Can Nuclear Forensics Trace a Detonated Nuclear Weapon." Scholars and scientists do not agree as to the effectiveness of such deceptive techniques, also called "spoofing." See Moody et al., *Nuclear Forensic Analysis*, 236–237, for a more skeptical stance.

¹⁸⁴ Talmadge, "Deterring a Nuclear 9/11."

¹⁸⁵ Miller, "Nuclear Attribution as Deterrence," 33.

¹⁸⁶ Phillips, "Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution."

Matthew Phillips analyzes a case of forensic analysis on uranium hexafluoride gas that Libya surrendered to the United States.¹⁸⁷ U.S. scientists claimed to be 90 percent certain that the samples were of North Korean origin, which “sparked a scientific and political controversy” when IAEA forensic scientists came to a different conclusion.¹⁸⁸ The debate appears to have stalled over questions of political influence and implications, and open-sources do not indicate a resolution. Kenton Moody provides a case study on an interdicted HEU sample in Bulgaria, which he claims as of 2001 was “the most thorough and far-reaching analysis of illicit nuclear material ever conducted.”¹⁸⁹ A team of scientists from several U.S. national laboratories actively analyzed the samples for over nine months, deriving many important signatures and narrowing the possible sources to reprocessing facilities serving HEU-powered research reactors. Although these scientists were almost certain that this HEU sample was produced somewhere in Europe, no definite attribution claim could be made as to the material’s source due to a lack of any database matches.¹⁹⁰ These cases illustrate the difficulty and complexity of nuclear forensic analysis, both of which would only intensify under the enormous time pressure following an actual terrorist nuclear attack.

A nuclear forensics capability does not guarantee successful attribution any more than having the ability to analyze fingerprints or DNA samples guarantees the identification of a criminal. What is important, however, is that the capability to perform nuclear forensics exists and is being further developed, and that the existence of a forensics-based attribution capability is well publicized to provide additional deterrence against acts of nuclear terrorism. I will now examine in greater detail the components that make up a forensics-based attribution capability, highlighting areas in which the United States needs to focus more effort.

¹⁸⁷ Phillips, “Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution,” 434–435.

¹⁸⁸ Ibid.

¹⁸⁹ Moody, *Nuclear Forensic Analysis*, 401–419.

¹⁹⁰ Ibid.

D. PROGRAM COMPONENTS

1. Scientific Limitations and Requirements

Specialized equipment is necessary in order to gather and then analyze evidence after a nuclear detonation. Personnel wearing protective gear will be able to gather samples at a safe distance from the point of detonation; robots are needed within a certain range due to intense initial heat and radiation. Aerial collection is possible using specially outfitted aircraft.¹⁹¹ The highly sophisticated equipment needed for analysis is located at several national laboratories, though some field instrumentation exists that could provide more expedient results.¹⁹² Equipment, of course, does not provide the answers on its own—the right personnel are required as operators.

A sufficient number of able, qualified, and available scientists is a core requirement for a nuclear forensic capability. The highly complex and labor-intensive nature of an iterative nuclear forensic investigation cannot be overstated. The scientists qualified to conduct such investigations hold advanced postgraduate academic degrees in such disciplines as chemistry, geochemistry, radiochemistry, nuclear physics, radiation physics, and nuclear engineering.¹⁹³ The current staffing requirement for these highly trained and experienced scientists at the national laboratories is estimated to be 75 positions.¹⁹⁴ Additionally, since the workforce market is not self-regulating at the present time, robust university and governmental programs are required that will ensure a continuing supply of the necessary brainpower.

The current U.S. capacity in regard to scientific requirements is only barely adequate; additionally, serious warning signs, both in equipment and personnel aspects, cast doubt on the long-term future. The Air Force currently maintains two WC-135 “Constant Phoenix” airplanes capable of recovering radioactive particles in the

¹⁹¹ Broad, “Addressing the Unthinkable, U.S. Revives Study of Fallout.”

¹⁹² Moody et al., *Nuclear Forensic Analysis*, 332.

¹⁹³ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 20.

¹⁹⁴ *Ibid.*

atmosphere following a nuclear detonation.¹⁹⁵ These aircraft are approaching fifty years old. Existing laboratory analysis equipment is sufficient, yet field analysis instrumentation is lacking.¹⁹⁶ Kenton Moody highlights his negative experience with such field equipment, stressing the importance of faith in the right people over faith in semi-automated machine analysis.¹⁹⁷ The national labs lack sufficient numbers of the right scientists, numbers that will continue to decline due to upcoming retirements and career-furthering transfers.¹⁹⁸ Student enrollment in university graduate radiochemistry programs has dwindled; in fact, less than six doctoral degrees in radiochemistry are granted each year nationwide.¹⁹⁹ Alarming, no comprehensive interagency plan exists to guide a national effort in addressing this personnel shortage.²⁰⁰ If the United States desires a lasting attribution capability, these present and future deficits in equipment and personnel must be urgently addressed.

2. Nuclear Materials Database

Because an attribution claim is strengthened when forensic data has been matched to an empirically derived signature, many analysts and leaders in the field call for the establishment of an international nuclear materials database.²⁰¹ Michael Miller agrees that a global database would be an ideal solution, but suggests achieving a comprehensive database is unlikely due to the tremendous political and technical obstacles involved.²⁰² I

¹⁹⁵ U.S. Air Force, "Factsheets: WC-135 Constant Phoenix," <http://www.af.mil/information/factsheets/factsheet.asp?fsID=192>.

¹⁹⁶ Moody et al., *Nuclear Forensic Analysis*, 332.

¹⁹⁷ Ibid.

¹⁹⁸ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 20.

¹⁹⁹ Ibid.

²⁰⁰ Aloise, Gene, *Nuclear Forensics: Comprehensive Interagency Plan Needed to Address Human Capital Issues*, GAO-09-527R (Washington, DC: U.S. GAO, 2009), 3.

²⁰¹ Michael May (director emeritus of the Lawrence Livermore National Laboratory), Jay Davis (former director of the Defense Threat Reduction Agency), and Raymond Jeanloz (chair of the National Academy of Sciences' Committee on International Security and Arms Control) make their case in May et al., "Preparing for the Worst." Many additional scholars cite this article while echoing the argument; see for example Levi, *Detering State Sponsorship of Nuclear Terrorism*, 26; Phillips, "Uncertain Justice," 432.

²⁰² Miller, "Nuclear Attribution as Deterrence," 50–51.

will now describe what such an ideal database would entail before qualifying the current U.S. and worldwide capability and highlighting some of the more difficult obstacles to successful achievement of the ideal.

The perfectly comprehensive database would include data on all known nuclear explosive materials as well as a library of physical samples of said materials.²⁰³ This data would include key elemental, isotopic, and physical properties of plutonium and HEU.²⁰⁴ Since each step of the nuclear fuel cycle changes signatures from previous steps, an exhaustive database would require validated signatures from the entire life cycle of plutonium and enriched uranium.²⁰⁵ The ideal data bank would include information and samples from nuclear-weapon states and non-nuclear-weapon states alike, from research, power, and weapons-fuel reactors, and from all phases of the uranium enrichment process. Although the prospect of assembling and maintaining such a database is truly daunting, the payoff in attribution credibility would be immense. Before estimating the feasibility of achieving such a database, it is necessary to describe the current situation and the obstacles to success.

Although numerous nuclear materials databases exist in the United States and various other countries, none of these approaches the level of comprehensiveness necessary for credible attribution.²⁰⁶ The U.S. Department of Energy maintains a database with considerable information on uranium compounds.²⁰⁷ Some U.S. and foreign laboratories, certain private entities, and the IAEA have physical sample libraries, but these are limited in scope.²⁰⁸ Some unilateral efforts are underway; for example, a new position was created at the Lawrence Livermore National Laboratory for a nuclear engineer to manage an attribution database.²⁰⁹ Other efforts are multilateral in nature.

²⁰³ May et al., “Preparing for the Worst,” 907.

²⁰⁴ Ibid.

²⁰⁵ Ferguson, “Can Nuclear Forensics Trace a Detonated Nuclear Weapon to its Source?” 5–6.

²⁰⁶ May et al., “Preparing for the Worst,” 907.

²⁰⁷ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 20.

²⁰⁸ Ibid.; see also May et al., “Preparing for the Worst,” 907.

²⁰⁹ Miller, “Nuclear Attribution as Deterrence,” 59, Note 51.

The Nuclear Smuggling International Technical Working Group, an independent association of nuclear forensics scientists, is working with Central Asian and other nations to assemble a database of both data and samples.²¹⁰ How well would such non-comprehensive databases function during an actual post-detonation forensic investigation?

Most scholars believe that the chances of reaching a credible attribution conclusion using currently available databases during an actual post-detonation investigation are low. Michael May et al. characterize the IAEA database as “incomplete and not designed for the event-driven rapid forensics ... required in response to a terrorist detonation.”²¹¹ Matthew Phillips asserts that “existing libraries of data are more likely to help identify a stolen nuclear weapon than one improvised by terrorists using fissile material.”²¹² Michael Miller points out that, although certain sources may be excluded and the search narrowed, without a matching sample a single perpetrator could not be singled out.²¹³ Given this pessimistic picture of attribution capability in light of the currently less-than-comprehensive nuclear materials databases, the desire for a comprehensive database should be evident. However, the obstacles are formidable.

Most of the obstacles to building a comprehensive international database of fissile materials information and samples are political in nature, though certain technical limitations are factors as well. Many scholars agree that due to the heavy secrecy placed on state weapons programs as well as commercial-use fuel and reactors, comprehensive information-sharing with an international organization is not likely to be easily

²¹⁰ David K. Smith, “International Nuclear Forensics as Part of a National Program to Safeguard Nuclear Materials,” Paper prepared for the American Association for the Advancement of Science 2008 Annual Meeting, Boston, MA, February 16, 2008, <http://cstsp.aaas.org/files/dksmith.pdf>, 16.

²¹¹ May et al., “Preparing for the Worst,” 907.

²¹² Phillips, “Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution,” 432.

²¹³ Miller, “Nuclear Attribution as Deterrence,” 41.

achieved.²¹⁴ Technical constraints include both the sheer volume of additional data to be obtained, as well as the inability to determine whether a given state has been forthcoming with all of its data and sample material.²¹⁵

Several proposals have been made to lessen some of these obstacles. William Dunlop and Harold Smith call for the formation of a team of experts with a special mandate granting worldwide pre-attack access to data and samples and immediate post-attack access to debris.²¹⁶ Michael May et al. propose establishing a fairly complex database consisting of a public component, in which sufficient information is revealed so as to build confidence in the veracity of the source, and a classified component, which could be interrogated only at a time of need by vetted analysts.²¹⁷ This database could be supplemented by challenge inspections similar to those incorporated in IAEA's "Additional Protocol."²¹⁸ Michal Miller contends that a comprehensive database invites cheating by states, which might surreptitiously withhold or manipulate data and samples, and would thus create a false sense of security.²¹⁹ He proposes, instead, a voluntary database, the goal being to establish a credible starting point while knowing there are knowledge gaps to fill.²²⁰ The more countries that participate in a voluntary database, the greater the pressure would be on any holdouts to join.²²¹ An important consideration to bear in mind for all of these proposals is that they only provide partial solutions to

²¹⁴ Dunlop and Smith, "Who did It?" 8; May et al., "Preparing for the Worst," 908; Miller, "Nuclear Attribution as Deterrence," 50–51.

²¹⁵ Miller, "Nuclear Attribution as Deterrence," 51.

²¹⁶ Dunlop and Smith, "Who did It?" 8.

²¹⁷ May et al., "Preparing for the Worst," 908.

²¹⁸ Ibid.

²¹⁹ Miller, "Nuclear Attribution as Deterrence," 51. The manipulation of material samples, often referred to as "spoofing," is technically very difficult and liable to exposure via the forensic process. Whether or not states might attempt to spoof, their prognosis for success, and means for combating it are debated. For more on this subject, see Phillips, "Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution," 431; May et al., "Preparing for the Worst," 908; Moody et al., *Nuclear Forensic Analysis*, 236–237.

²²⁰ Miller, "Nuclear Attribution as Deterrence," 51.

²²¹ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 26.

what amount to complex political problems, both domestically and internationally. To implement any of them would require a considerable amount of political capital and international leadership.

3. Intelligence Support

The United States has been collecting intelligence information on other states' nuclear weapons and energy programs since World War II with mixed success, and requirements driving the intelligence effort have only become broader in the post-Cold War world. Although it is not possible to define precise intelligence requirements with regard to an attribution capability, I here attempt to paint a rough picture of current intelligence support based, in part, upon recent events, as well as to highlight some recommendations for the future. The intelligence needed to support an attribution capability can be broken down, roughly, into two areas. The first of these areas comprises efforts to bolster existing U.S. nuclear databases. The second, much broader in scope, can be thought of as "classical" intelligence support, and includes the collection and analysis of any information regarding the nuclear capabilities and intentions of states and terrorist groups, as well as information regarding terrorist activities or plots. Intelligence from either of these two areas could be used to add significant credibility to any attribution claim.

Intelligence efforts to bolster existing nuclear databases may be provided through various means, to include "human intelligence" (HUMINT), and "measurement and signature intelligence" (MASINT). The CIA has responsibility for most foreign HUMINT efforts, though DoD and the FBI have increased their recent activity in this domain.²²² Since 1973, the overall MASINT effort regarding foreign nuclear detonations has been the responsibility of the Air Force Technical Applications Center (AFTAC).²²³ AFTAC has developed and oversees multiple sensory arrays designed to detect nuclear

²²² The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, DC, 2005).

²²³ AFTAC Public Affairs, "Air Force ISR Agency—AFTAC," <http://www.afisr.af.mil/units/aftac.asp>; Richelson, *Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea*, 538.

explosions as well as collect various signatures inherent in nuclear events.²²⁴ The extent to which these and other efforts contribute to the expansion of U.S. nuclear databases, if at all, as well as their degree of success in this regard is classified. However, one report does suggest the insufficiency, underfunding, and underutilization of MASINT resources.²²⁵ Regardless, it is impossible to quantify either specific requirements or results. Absent a comprehensive nuclear database, efforts should be made in this area to increase the extent of existing databases.

The challenge facing the Intelligence Community (IC) in providing intelligence on the nuclear capabilities and intentions of states and terrorist groups is enormous. Various commissions and reports provide insight into recent IC failures and successes, as well as advocate many possible reforms and initiatives for bolstering future performance.

In its *Report to the President of the United States*, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction found that “the Intelligence Community knows disturbingly little about the nuclear programs of many of the world’s most dangerous actors.”²²⁶ These actors specifically include “Iran, North Korea, China, and Russia.”²²⁷ Regarding the erroneous pre-war assessment of Iraq’s WMD programs, what it called “one of the most ... damaging intelligence failures in recent American history,” the Commission faulted both intelligence analysts and collectors from CIA, the Defense Intelligence Agency, the National Security Agency, and the National Geospatial-Intelligence Agency.²²⁸ Although it singled out IC successes in collection and analysis with regard to Libya’s WMD programs as well as the A.Q. Khan network, the Commission concluded that the IC’s collection strategies are insufficient both in scope and coordination to penetrate the myriad of potential targets today.²²⁹

²²⁴ Richelson, *Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea*, 538.

²²⁵ The Commission on the Intelligence Capabilities of the United States, *Report to the President*, 23.

²²⁶ *Ibid.*, 4.

²²⁷ *Ibid.*, 11.

²²⁸ *Ibid.*, 3.

²²⁹ *Ibid.*, 11–12.

A U.S. House committee report decries the gaps in the IC's collection coverage regarding Iran's WMD programs, both in terms of the Iranian program's current status, and in providing actionable intelligence that would allow the denial of material support to the Iranian program.²³⁰ The report also emphasizes the need for greater insight into the inner-workings and intentions of the Iranian government, as well as the nature of its links to and support for terrorist groups.²³¹

These and other studies propose numerous suggestions for improvement. The need to improve HUMINT capabilities almost always makes such lists, as does improving IC internal and external coordination.²³² Other reports point out the paucity of language and technical skills amongst both collectors and analysts and emphasize the importance of correcting such deficits.²³³

This brief overview of recent IC failures, successes, and recommendations for improvement indicates the daunting task before the IC, depicts the current shortfalls in capabilities, and provides a qualitative picture of general future requirements. Nuclear forensics cannot function alone—without robust intelligence support, nuclear forensic analysis will not provide policymakers the credibility necessary for definitive action.

4. Law Enforcement Support

While support from the Intelligence Community is crucial to the success of an attribution program, law enforcement support actually provides the framework from which an attribution program may operate. Such a framework should ideally be composed of vetted procedures for evidence gathering and transport, processing protocols, laboratory standard and best practices, evidence analysis techniques, and

²³⁰ U.S. House of Representatives, Permanent Select Committee on Intelligence, *Recognizing Iran as a Strategic Threat: An Intelligence Challenge for the United States*, Washington, DC: U.S. House of Representatives, 2006, <http://intelligence.house.gov/media/pdfs/iranreport082206v2.pdf>, 16–17.

²³¹ *Ibid.*, 19–23.

²³² The Commission on the Intelligence Capabilities of the United States, *Report to the President*, 21–37; U.S. House of Representatives, *Recognizing Iran as a Strategic Threat*, 24–25.

²³³ Graham et al., *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, 99–100; Defense Science Board Task Force, *Nuclear Deterrence Skills* (Washington, DC: Office of the Under Secretary of Defense, 2008), 44–45.

ultimately, the determination of evidentiary standards for credible attribution.²³⁴ I now briefly highlight a few of the programs and initiatives underway, and emphasize future support requirements from the law enforcement community.

The FBI, as the designated lead federal agency for investigating terrorist acts in the United States, manages and coordinates the preparation for and execution of all WMD investigations.²³⁵ The leader in the field of traditional forensics analysis, the FBI continues to utilize that core skill set while directing overall nuclear and radiological forensic investigations.²³⁶ The FBI has recognized its leadership and centrality in the attribution process by establishing several important interagency procedural and training initiatives.

According to 2007 Congressional testimony by Dr. Vahid Majidi, then Assistant FBI Director for the Weapons of Mass Destruction Directorate, the FBI Laboratory Division is “central” to interagency nuclear forensics efforts.²³⁷ The Laboratory boasts a Hazardous Materials Response Unit, composed of 27 teams of personnel and associated equipment located throughout the United States, that provides WMD “crime scene awareness” training to personnel across the interagency. The Laboratory’s Chemical Biological Science Unit directs nuclear forensics investigations, working by formal agreement in conjunction with other U.S. government labs as well as AFTAC to analyze both pre- and post-detonation samples. Additionally, the Laboratory has overcome the obstacles to performing traditional forensic analysis on contaminated particles by training its traditional analysts to operate in WMD laboratories. Many of these innovative programs and procedures are precedent setting, both domestically and internationally.

²³⁴ Robert McCreight and Stanley Supinski, “Post-Strike Attribution-A Political & Scientific Dilemma,” *Journal of Homeland Security and Emergency Management* 4, no. 2, article 11 (2007), <http://www.bepress.com/jhsem/vol4/iss2/11/>, 4.

²³⁵ Federal Bureau of Investigation, “Weapons of Mass Destruction Homepage,” http://www.fbi.gov/hq/nsb/wmd/wmd_home.htm.

²³⁶ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 36.

²³⁷ Vahid Majidi, Written Testimony before the U.S. House of Representatives Homeland Security Committee, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, October 10, 2007, <http://homeland.house.gov/SiteDocuments/20071010175326-18735.pdf>. All subsequent information in this paragraph comes from this source.

More must be done, both unilaterally and otherwise. Standards are still lacking in many areas of the attribution process.²³⁸ Significant gains have been made with regard to international cooperation, yet agreed-upon universal procedural standards do not exist.²³⁹ Most significantly, the difficult problem of determining evidentiary standards has not been settled.²⁴⁰ While it can be argued that the degree of attribution “confidence” required for follow-on action is strictly a political determination, the law-enforcement, intelligence, and scientific communities must together determine “what amount of evidence, what degree of specificity, what scale of incriminating data, and what overall level of persuasive and circumstantial facts and theories enable a final [attribution] determination to be made.”²⁴¹ Though related, the determination of evidentiary standards should inform the more complex political determination.

The law-enforcement community understands the complex challenges it faces regarding nuclear forensics and appears to be making progress in achieving some degree of resolution on the easier issues. However, much remains to be done regarding the formidable challenges of building domestic and international consensus on procedural and evidentiary standards. Such consensus-building will continue to present challenges, for one, due to the sheer number of organizations and agencies involved in the attribution process. The discussion now turns to the task of exercising the response of these numerous organizations.

²³⁸ McCreight and Supinski, “Post-Strike Attribution-A Political & Scientific Dilemma,” 4.

²³⁹ The International Atomic Energy Agency published “Nuclear Forensics Support” in 2006, a groundbreaking manual as part of the *IAEA Nuclear Security Series* intended to “provide national policy makers, decision makers and technical managers with consolidated guidance for responding to incidents involving the interdiction of nuclear and other radioactive material, when nuclear forensic investigations are required.” (p. 1). This publication provides a valuable starting point for the discussion regarding pre-detonation forensics; post-detonation forensics adds additional considerations and challenges to the procedural basis outlined therein.

²⁴⁰ McCreight and Supinski, “Post-Strike Attribution-A Political & Scientific Dilemma,” 4.

²⁴¹ *Ibid.*

5. Exercise Requirements

Myriad governmental agencies at various levels play important roles in the attribution process, among them DoE, DHS, DoJ, DoD, DoS, and the IC.²⁴² Given the potentially catastrophic consequences of a terrorist nuclear attack and the ensuing chaos, each of these agencies and their involved sub-organizations must have a thoroughly practiced understanding of their roles.

The Tier 1 National Level Exercise series (formerly known as TOPOFF), mandated by Congress, has been valuable in exercising these multiple agency roles and serving to better prepare personnel ranging from senior government officials to mid-level bureaucrats to first-responders.²⁴³ The Department of Homeland Security sponsored TOPOFF-4, a two-year series of seminars, planning, and exercises called the “most comprehensive terrorism exercise ever conducted in the United States.”²⁴⁴ Various other exercises specific to the technical challenges of post-detonation attribution have been created by DoD, DoE, FBI, and the IC.²⁴⁵

Although the frequency and extent of exercises to date has been sufficient overall, some scholars point out that the exercises specifically relating to the challenges of post-detonation attribution have stressed the technical component over high-level decision-making.²⁴⁶ Officials at the highest levels of government must be challenged to integrate all available information in the time frame that it would likely be provided them and make difficult attribution-based decisions all while managing public expectations for quick, forceful action.²⁴⁷ High-level comprehensive exercises should instill in policy- and decision makers a truer sense of what is currently possible in the field, as well as

²⁴² For an overview of the key players and their roles, see Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 36–38.

²⁴³ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 38.

²⁴⁴ U.S. Department of Homeland Security, “Office of Grants and Training—Exercises,” <http://www.ojp.usdoj.gov/odp/exercises.htm> (accessed June 5, 2009).

²⁴⁵ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 30.

²⁴⁶ Ibid.

²⁴⁷ Ibid.

provide impetus for increased investment, should that be deemed necessary.²⁴⁸ The pieces are in place, domestically, to establish such exercises today. Since the credibility of any attribution claim would increase with international consensus, the number of exercise participants should be expanded as international partners join the post-detonation forensics-based attribution effort.

E. COSTS TO IMPROVE AND SUSTAIN

In light of this long, and yet not exhaustive, list of program needs, I now briefly characterize the likely costs necessary to achieve certain program improvements. I assess financial and political costs qualitatively, ultimately posing the fundamental question: Should the United States be willing to pay these costs?

Not all problems can be solved by simply “throwing” more money at them; however, money wisely invested can be a powerful tool on the road to success. A bill being considered by the U.S. Senate as of October 2009, HR 730, would provide \$30 million per year over the next three fiscal years to create and fund programs within the DHS Domestic Nuclear Detection Office intended to improve pre- and post-detonation nuclear forensics capability, stimulate and bolster the nuclear forensic science academic pipeline, and create an office for centralized planning and coordination of all national nuclear forensics activities, to include exercises.²⁴⁹ Of course, in a national budget of nearly \$4 trillion for 2009, \$30 million is a relatively small number, and will not go far in a complex, technology-laden research and development effort. Indeed, only 0.005 percent of all nuclear weapons-related expenses are designated for nuclear forensics technology development.²⁵⁰ Graham Allison estimates that a “total war” on nuclear terrorism, “our highest [defense] priority,” would cost from \$5 billion to \$10 billion per

²⁴⁸ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 30.

²⁴⁹ *U.S. Fed News Service, Including U.S. State News*. “Rep. Thompson Issues Statement in Support of Nuclear Forensics and Attribution Act,” March 25, 2009; U.S. Congress, “H.R. 730—Nuclear Forensics and Attribution Act.”

²⁵⁰ Stephen I. Schwartz and Deepti Choubey, *Nuclear Security Spending: Assessing Costs, Examining Priorities* (Washington, DC: Carnegie Endowment for International Peace, 2009), 34.

year, which he equates to “a penny of every dollar” of the current defense budget.²⁵¹ Clearly, though funds are not unlimited, the field of nuclear forensics and event attribution should be granted higher fiscal priority.

Granting higher fiscal priority to nuclear forensics and event attribution is problematic, however, since “the nation’s nuclear forensics capabilities depend heavily on the continued funding of equipment, infrastructure, and personnel currently paid for by other programs.”²⁵² Although the four agencies with primary responsibility for implementing the National Technical Nuclear Forensics program (DoD, DoE, DHS, FBI) spent or will spend approximately \$60 million in 2008 and \$59 million in 2009, the program’s true costs are higher due to its dependence on resources not reflected in these budgets.²⁵³ Thus, precise long-term fiscal needs are undetermined; effective resource allocation and program prioritization will be difficult until these true costs are fully ascertained.²⁵⁴

A well-known principle of economics states that since resources are scarce, any expenditure incurs an opportunity cost. In other words, financial and political capital dedicated to nuclear forensics and event-attribution program development will not be available for other programs. For example, scientists researching and developing nuclear forensics technology are not available for the research and development of detection equipment and programs intended to prevent the incursion of nuclear materials or weapons into the United States; money spent upgrading forensics equipment is not available for improving detection technology. These examples notwithstanding, most opportunity costs regarding nuclear forensics-based attribution development are likely political in nature.

As referenced above, enormous political capital is required in order to overcome obstacles to information sharing and building an international database along with

²⁵¹ Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 177.

²⁵² U.S. Government Accountability Office, *Nuclear Forensics: Comprehensive Interagency Plan Needed to Address Human Capital Issues*, 9.

²⁵³ *Ibid.*, 8.

²⁵⁴ *Ibid.*, 9–11.

forensics procedures. This political capital would have to be spent by those that have it—those at the highest levels of the U.S. government. Whether or not these lofty goals can be achieved is debatable. In the attempt to realize goals, furthering a national or international nuclear forensics-based attribution capability other “opportunities” might suffer.

Many important nuclear-related programs require political attention: The Proliferation Security Initiative should be expanded; the Comprehensive Test Ban Treaty has never been ratified by the U.S. Senate and, as such, cannot enter into force; a Review Conference for the Nuclear Nonproliferation Treaty takes place in 2010 with important issues at stake; the IAEA’s “Additional Protocols” have not been adopted by all states; increased international support for the Reduced Enrichment for Research and Test Reactors Program should be solicited; and programs such as the Cooperative Threat Reduction program and the Global Threat Reduction Initiative would benefit from increased multilateral cooperation. Each of these requires a large degree of political effort to maintain or improve. President Obama’s ambitious goal of eliminating world nuclear weapon stockpiles may be considered in a more difficult political category altogether, as can counter-proliferation efforts regarding North Korea and Iran. Determinations of whether pursuing some of the aforementioned might mutually reinforce the goals of a nuclear forensics-based attribution program or prove detrimental is outside the scope of this thesis. It is sufficient to say, generally, that time and energy spent on any given program is time and energy not available for another. Political leaders must balance their available political capital with prospects for any given program’s advancement in determining international engagement priorities.

F. CHAPTER SUMMARY

The national capability to attribute a nuclear terrorist attack today is not assured; the program falls short of the ideal in several identifiable ways. Although progress is being made in terms of improving scientific capacity, nuclear databases, intelligence support, law-enforcement support, and exercise programs, much more remains to be done. As shown in Chapter III, a perfect attribution capability is not required for an

effective deterrent posture. If a potential state sponsor believes that it would *probably* be positively identified, deterrence functions well. Given the current state of the program, a potential state sponsor may not come to such a conclusion; thus, current U.S. attribution capability with regard to reliability and accuracy for deterrence purposes seems insufficient. Although expensive, primarily politically and in terms of lost opportunities, this capability could be increased to a sufficient level in the long term.

Should the U.S. government be willing to pay the significant costs required to increase its attribution capability? In light of the risk of attack as assessed in Chapter II, as well as the benefit that the role of attribution-enabled deterrence provides as described in Chapter III, the answer is a qualified “yes.” The risk assessment shows that the situation is neither dire, nor can the threat be ignored. Attribution-enabled deterrence fills a critical strategy gap for preventing nuclear terrorism, but its relatively narrow application highlights the equal importance of complementary strategic programs. As such, money and political capital must be expended across a spectrum of important programs. Political focus is required to ensure the best investment of scarce fiscal and political resources both for the short and long term. By ensuring that the government gets the most “bang for the buck,” national decision makers can build and sustain an attribution program sufficient to enable credible deterrence. In the next chapter, I make additional specific policy recommendations with regard to program investment.

V. CONCLUSION

In this thesis, I have explored several aspects of the United States' nuclear forensics-based post-detonation attribution program and its role in deterring state sponsorship of nuclear terrorism, with the ultimate goal of determining whether the nation is "on target" in its efforts. In particular, I have explored questions and made assessments regarding the following: 1) the importance of the program in preventing nuclear terrorism; 2) the levels of program reliability and accuracy necessary for effective deterrence; 3) the most appropriate attribution-enabled deterrence posture, as well as the credibility of this posture; 4) the specific role of nuclear forensics in the U.S. attribution program as well as the overall state of the program; and, 5) an approximation of the investment required to close the critical gap between current and desired attribution performance. I now review key findings from earlier chapters relating to these points before making overall policy recommendations.

A. REVIEW OF KEY FINDINGS

1. Importance of an Attribution Program

The risk assessment of Chapter II demonstrates that the threat component of nuclear terrorism is very low, primarily due to the exceedingly high barriers to terrorist acquisition of a nuclear capability. The risk, however, remains significant due to the potentially enormous consequences of a nuclear attack, as well as the relatively high level of U.S. vulnerability to attack. Furthermore, the risk assessment shows that one of the most effective current means for mitigating risk is by further reducing the probability that a terrorist group might achieve a nuclear capability. Because it directly enables the deterrence of state sponsorship of nuclear terrorism, an attribution capability provides an essential means for reducing this probability. In the absence of an attribution capability, any deterrence-by-punishment threat would strain credibility; additionally, potential state

sponsors might be encouraged by the likelihood of remaining anonymous. Thus, forensics-based attribution plays a critical role in preventing nuclear terrorism. The United States rightly desires a robust attribution capability.

2. Reliability and Accuracy Necessary for Effective Deterrence

As noted in Chapter I, the United States has seemingly acknowledged having only an emerging forensics-based attribution capability. If deterrence depends on a perfect attribution capability, the United States has issued deterrent threats in vain. This is not the case, however. The analysis in Chapter III shows that although the capability to determine the source of an attack is the crux of the credibility problem, perfect attribution, while desirable, is not required. A deterrent threat to retaliate explicitly based on strong, but not perfect, evidence would force an accused state to demonstrate that it was not involved; this effectively splits the burden of proof and compensates for an imperfect attribution capability.

This uncertainty of attribution might have different effects on different states. To the degree that states are satisfied with the status quo they will likely not be risk tolerant; hence, any chance of being found complicit in a nuclear attack should provide sufficient deterrence. Conversely, deterring states dissatisfied with the status quo and therefore more risk tolerant might require a greater attribution capability.

3. The Appropriate Deterrence Posture and Its Credibility

The analysis of deterrence theory in Chapter III indicates that an inviolable redline should be broadly established to deter the purposeful transfer of nuclear materials or weapons to terrorists; this line should only be shifted to include unintentional transfer in certain situations and for specific actors. The translation of this actor-specific concept into strategy reveals a somewhat narrow application for attribution-enabled deterrence. Only those few adversarial states that possess nuclear weapons or fissile materials that may potentially sponsor terrorist groups, and with whom the real potential for security cooperation is nonexistent should be specifically targeted with deterrence of both purposeful and unintentional transfer.

Deterrence can be strengthened in several ways. The United States must be careful not to force its adversaries into a losses frame of reasoning by coercively maintaining an undesirable status quo. Additionally, since a specific threat to retaliate with nuclear weapons might be perceived as unjustly punishing innocent civilians, credibility can be best maintained by ambiguously threatening a severe response. This leaves all options available, yet pointedly reserves the right to respond severely and in kind. Credibility also increases proportionately with the strength of the U.S. attribution program, since even reducing the degree of attribution confidence by splitting the burden of proof requires strong evidence against any given state.

4. Role of Nuclear Forensics and Overall State of Attribution Program

Chapter IV demonstrates that although nuclear forensics occupies the central role in a post-attack attribution program, it cannot bear the burden alone. For an attribution program to function well and provide credible results, the intelligence and law enforcement communities must support nuclear forensic analysis. Accurate forensic results depend upon highly specialized scientists operating state-of-the-art equipment and relying on the availability of informational and material databases. Additionally, due to the technical and organizational complexity of the attribution process, a national attribution skill-set must be systematically exercised and evaluated in order to develop and maintain any given capability level.

Much positive work has been accomplished toward developing the U.S. attribution program; however, shortfalls exist in key areas. The understaffing of the scientific workforce at the heart of nuclear forensic analysis is projected to increase without focused governmental stimulus efforts. Existing nuclear databases are insufficient. Intelligence support should be strengthened, as should the framework provided by the law enforcement community. Without sufficient government attention and resources devoted to these key areas, the nation's attribution capability, already falling short of the ideal, will certainly atrophy. The United States should not be

confident that its attribution program is currently sufficiently developed so as to credibly deter state sponsorship of nuclear terrorism, and should take steps to increase a potential state sponsor's belief that it would be exposed.

5. Costs to Close the Gap

The investments required to improve the U.S. attribution program can be categorized as either financial or political, and encompass both direct and opportunity costs. The need for increased direct funding is most easily addressed, but even this is complicated by the plethora of different executive agencies involved in the attribution effort. Financial resources must be smartly managed with an emphasis on long-term program needs. The most tangible financial opportunity costs in this area center around the employment of the nation's nuclear scientists—those dedicated to nuclear forensics are not available to work on other nuclear national priorities.

Political costs, both direct and in terms of opportunity, are difficult to qualify. Many different programs compete for priority and the necessary political attention, both domestically and in the international arena. The political capital required in overcoming obstacles to creating an international database and establishing a multilateral nuclear forensics regime would likely be immense. Since the political capital required to advance an international attribution regime might work to further other ambitious multilateral strategic goals, more research is needed to determine how to employ such political capital to best effect, as well as to qualify prospects for ultimate success.

B. OVERALL POLICY RECOMMENDATIONS

I have reserved this section of my thesis only for those policy recommendations that I feel are of the most pressing immediate priority. Additional recommendations have been made throughout the thesis itself, and the fact they are not repeated here does not imply that they should be ignored in the long term. In the most general sense, the United States should focus first on getting its own attribution “house” in order. This is not to say that current international coordination efforts should cease—only that high-level political capital should be preserved and spent at such a time when the United States is confident

in all aspects of its own attribution program, knows the clear way forward, and can realistically achieve a high level of return for its investment.²⁵⁵ I now recommend several ways in which the United States can maximize its current attribution capability, invest for the future, and assume an appropriate deterrence posture.

1. Current Capability Maximization

The United States should maximize its existing attribution capability by instituting two relatively minor shifts in the execution of current policy. First, the government must publicly assert the existence of a reliable attribution capability.²⁵⁶ This can be done, in part, by removing contradictory or misleading statements from its strategy documents. For example, a sentence in the 2006 National Strategy for Combating Terrorism states, “We will develop the capability to assign responsibility for the intended or actual use of WMD via accurate attribution,”²⁵⁷ this could be replaced with the following more convincing statement, “We will continuously improve upon our existing capability to assign responsibility.” The suggested wording is not untruthful—the United States does possess an attribution capability, however imperfect. In support of this public assertion of an attribution capability, attribution program successes, whether from forensics performed on interdicted fissile material or from exercises, should be publicized through scientific and other available channels.²⁵⁸ This is not to suggest that the United States should exaggerate its capabilities; embellishment might either seem incredible to adversaries or lead to unrealistic public expectations in the event of an attack. As the United States projects confidence in its attribution program and supports this confidence with actual successes, the credibility of deterrent threats will be strengthened.

Another way in which the government can maximize its current capability is by improving the design of current national-level exercises. By putting greater emphasis on

²⁵⁵ Such an approach would suggest, for example, the continued pursuit of unilateral nuclear-materials databases over currently unfeasible multinational databases.

²⁵⁶ Talmadge, “Deterring a Nuclear 9/11,” 30.

²⁵⁷ Office of the President, *National Strategy for Combating Terrorism*, 15.

²⁵⁸ Talmadge, “Deterring a Nuclear 9/11,” 30.

the high-level decision-making, interagency, and multinational aspects of periodic technical forensics-based attribution exercises, government leaders at the highest levels can be educated regarding current attribution capability and be forced to exercise decision-making authority in a simulated complex and time-sensitive environment. Moreover, results from these exercises can be used to shape the interagency—and, eventually, international—standard operating procedures necessary to ensure the most efficient practices should the capability ever be called upon. By rehearsing various organizational and political challenges, the government would facilitate the development of valuable skill sets and interagency relationships at all levels, thus ensuring the best capitalization of its current attribution capability.

2. Investment for the Future

The United States must increase its investment in nuclear forensics-based attribution. Since the risk of nuclear terrorism is real, an attribution capability occupies an essential position in the nation's counterterrorism strategy both for enabling deterrence and for the prevention of follow-on attacks. Without higher-priority funding and political attention, this necessarily complex program will fail to reach and maintain a sufficient capability level. How can better funding and political emphasis be accomplished in a reality of scarce resources and competing priorities?

The U.S. government must balance critical program needs with the fiscal and political investments that would yield the greatest long-term return for the least cost. The findings of this thesis indicate that the scientific personnel aspect of the nation's attribution program, more than any other, exhibits both short-term needs and the promise of long-term capability improvement. Without the requisite highly skilled scientists, each requiring years of education and experience, no amount of future investment can sustain or improve a forensics-based attribution program.

The United States must engage in a sustained, focused political effort in order to rectify the emerging crisis within the nuclear-forensics scientific community. A U.S. Government Accountability Office report, published in April 2009, recommends the Secretary of Homeland Security “develop a comprehensive interagency plan to address

the human capital deficiencies affecting the NTNF [National Technical Nuclear Forensics] program. This plan should include estimates of the long-term demand, from both the U.S. government and private industry, for trained personnel in key disciplines, such as radiochemistry, that support the NTNF program.”²⁵⁹ Additionally, a 2008 report by the Nuclear Forensics Working Group of the American Physical Society and the American Association for the Advancement of Science recommends government funding for university radiochemistry programs as well as specific programs designed to strengthen university-national laboratory interaction, to include fellowships, internships, and contract support.²⁶⁰ I fully endorse these recommendations, and add that such a government plan must include means for measuring the effectiveness of current and future efforts to bolster the national scientific pipeline. The government should periodically revisit plan estimates of supply and demand and tailor specific programs commensurately with any new findings.

3. Deterrence Posture

The United States should not employ a deterrence-of-negligence strategy for any international relationships in which cooperation exists to any degree regarding the security of fissile materials, and in which the other state is not a plausible sponsor of nuclear terrorism. Such a strategy would be counterproductive for two reasons: 1) this coercive threat would likely serve to hinder cooperation both before and after a terrorist nuclear attack; and 2) retaliatory threats based upon a negligence strategy stretch the limits of credibility when applied to cooperative, friendly states with nuclear weapons. This recommendation does not suggest discarding such a strategy for antagonistic states, or eliminating the possibility of post-detonation coercive pressure on an unintentionally offending state.

²⁵⁹ U.S. Government Accountability Office, *Nuclear Forensics: Comprehensive Interagency Plan Needed to Address Human Capital Issues*, 11.

²⁶⁰ Joint Working Group, *Nuclear Forensics: Role, State of the Art, and Program Needs*, 20–21.

By dismissing attempts to coerce already cooperative states into greater cooperation through deterrence of negligence, the focus of deterrence can be narrowed considerably to antagonistic states possessing nuclear weapons or fissile materials that may consider sponsoring nuclear terrorism. In today's world, North Korea presently fits that description, and Iran may as well in the relatively near future.

In dealing with North Korea, the United States should not be explicit regarding the nature of the promised consequences for sponsoring nuclear terrorism.²⁶¹ This is consistent with existing policy documents and statements ambiguously promising “overwhelming consequences.”²⁶² Although these threats hint at the perhaps incredible threat of nuclear retaliation, North Korea should not be given reason to doubt that the United States reserves the right to make any retaliation as painful as possible. Additionally, the United States should make explicitly clear to North Korea its intention to treat any transfer of North Korean fissile material or weapons as purposeful. This will preclude any post-detonation “excuses” on the part of North Korea to make such transfers appear accidental (truthful or not) and thus avoid retribution.²⁶³ In short, the United States should specify the undesired actions precisely to North Korea, yet communicate the threatened consequences with ambiguity.

4. For Further Research

More research should be done regarding actor-specific deterrence strategies as enabled by an attribution capability. Determining the impact of an imperfect attribution capability in deterring specific states and individuals within certain states would prove valuable. Each of these targets' risk tolerance and tendency to misperceive should be assessed; this, in turn, would facilitate more precise communication of both an attribution capability and the intent to respond. Certain targets and/or states might become the focus of specific intelligence-gathering operations intended to tailor and improve the U.S.

²⁶¹ Phillips, “Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution,” 442.

²⁶² Office of the President, *National Strategy for Combating Terrorism*, 14–15.

²⁶³ Levi, *Deterring State Sponsorship of Nuclear Terrorism*, 20.

attribution capability appropriately. Additionally, the United States could shift more of the burden-of-proof to certain hard-to-deter targets; this shift would, of course, have to be effectively communicated.

An accurate accounting of comprehensive attribution-program costs currently does not exist. Congress should request such a report and use the results as a basis for future investment decisions as well as a gauge for measuring returns on investment. Direct and indirect costs across the federal government must be included, with a focus on capturing costs for the infrastructure and personnel that provide program support yet are funded by different programs.²⁶⁴ This will maximize current resource utilization, present a clearer picture of future program funding needs, and ensure the attribution effort is not unintentionally harmed by reducing funding for now-hidden support aspects.

Further research is also needed to better evaluate both domestic and international political costs inherent to the nation's attribution program. Such research might take the form of a cost-benefit analysis, even attempting to assess the likelihood of achieving various politically challenging aspects of the program. Comparisons should be made across the range of government programs related to nuclear weapons policy or the prevention of nuclear terrorism in order to determine which programs might provide a mutual benefit to the attribution program, which might prove contradictory in some form, and which have no impact whatsoever. The results of such a study would prove invaluable to analysts and policymakers alike in determining which programs offer the best overall return on investment toward securing the nation from nuclear terrorism.

An additional important area for further research, and one that may be related to the cost-benefit analyses described above, is the determination of measures of effectiveness for various nuclear counterterrorism programs. For example, how effective is the GTRI in securing SNM stockpiles? How much security is “good enough” when compared with program costs and in light of the risk? Similarly, how can the effectiveness of the national forensics-enabled attribution program in providing a credible deterrence posture be measured? Perhaps most importantly—at what point do

²⁶⁴ U.S. Government Accountability Office, *Nuclear Forensics: Comprehensive Interagency Plan Needed to Address Human Capital Issues*, 10–11.

diminishing returns make the pursuit of further program development unfruitful? In an age of ever-scarcer resources, policymakers and decision makers at the highest levels of government must make difficult judgments regarding which areas require more focused efforts in light of the nation's risk tolerance. In order to make such decisions, they must be given accurate information as to any tradeoffs involved, as well as which programs would provide—or are already providing—the most tangible benefits.

Once the United States has maximized its own attribution capability, it should look for opportunities to strengthen the international attribution regime. Further research should be done into how this could best be accomplished. This research would have to address the political and technical difficulties presented by the biggest current obstacle to international cooperation—creating an effective international nuclear materials database. Case studies into past successes and failures regarding cooperative nuclear-policy regimes might be accomplished to determine how best to elicit international cooperation. A roadmap might emerge from such research, ultimately enabling policymakers to avoid common pitfalls as well as to best exploit opportunities for success.

C. CONCLUDING THOUGHTS

I agree neither with those authors who claim the risk of nuclear terrorism is extreme and that preventing it should be the highest national-security priority, nor with those who claim that the threat is overly exaggerated.²⁶⁵ To turn the cliché back around: it is a matter not of “when,” but “if.” Nuclear terrorism is a risk of both low probability and high consequences; therefore, the United States must diligently pursue the most effective, yet practical, means for mitigating this risk. Nuclear forensics-based attribution is one such means for risk mitigation, enabling both pre-attack deterrence of state sponsorship and post-attack response options. I have demonstrated herein the fairly

²⁶⁵ Graham Allison, Micah Zenko, and Matthew Bunn represent the former characterization, while John Parachini, Jessica Stern, Robin Frost, and John Mueller are members of the latter. See Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1–120; Zenko, “Intelligence Estimates of Nuclear Terrorism;” Bunn, “A Mathematical Model of the Risk of Nuclear Terrorism,” 103; Parachini, “Putting WMD Terrorism into Perspective,” 42–46; Stern, *The Ultimate Terrorists*, 10, 48–86; Frost, “Nuclear Terrorism after 9/11,” 7; Mueller, *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why we Believe them*, 14–17.

narrow, albeit valuable, application of attribution-enabled deterrence. I have also shown ways in which the U.S. attribution capability is lacking and have made suggestions for both current capability maximization and future improvements. A strong and improving post-detonation attribution capability would increase the credibility of U.S. deterrence, ironically making the actual use of such a capability less likely to be needed. Although the United States is currently investing both political and fiscal resources in its attribution capability, additional focus is needed to bring the effort more accurately “on target.”

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- AFTAC Public Affairs. "Air Force ISR Agency—AFTAC." <http://www.afisr.af.mil/units/aftac.asp> (accessed June 4, 2009).
- Albright, David, and Kimberly Kramer. "Fissile Material: Stockpiles Still Growing." *Bulletin of the Atomic Scientists* 60, no. 6 (November/December 2004): 14–16. http://www.isis-online.org/global_stocks/bulletin_albright_kramer.pdf (accessed September 24, 2009).
- Albright, David. "Al Qaeda's Nuclear Program: Through the Window of Seized Documents." *Nautilus Institute Policy Forum Online*. Special Forum 47 (November 6, 2002). http://www.nautilus.org/archives/fora/Special-Policy-Forum/47_Albright.html (accessed May 17, 2009).
- Allison, Graham. "Nuclear Deterrence in the Age of Nuclear Terrorism." *Technology Review* 111, no. 6 (November/December 2008): 68–73.
- _____. "The Only Thing that can Keep Nuclear Bombs out of the Hands of Terrorists is a Brand-New Science of Nuclear Forensics." *Newsweek* 153, no. 12 (March 23, 2009).
- _____. *Nuclear Terrorism: The Ultimate Preventable Catastrophe*. New York, NY: Times Books, Henry Holt and Company, LLC, 2004.
- Aloise, Gene. *Nuclear Forensics: Comprehensive Interagency Plan Needed to Address Human Capital Issues*. GAO-09-527R. Washington, DC: U.S. GAO, 2009.
- Auerswald, David P. "Deterring Nonstate WMD Attacks." *Political Science Quarterly* 121, no. 4 (Winter 2006): 543–568.
- Bennett, Drake. "Give Nukes a Chance: Can the Spread of Nuclear Weapons Make U.S. Safer?" *The Boston Globe*, March 20, 2005. http://www.boston.com/news/globe/ideas/articles/2005/03/20/give_nukes_a_chance/ (accessed May 17, 2009).
- Berejikian, Jeffrey D. "A Cognitive Theory of Deterrence." *Journal of Peace Research* 39, no. 2 (2002): 165–183.
- Bleek, Phillip C. "Would 'Deterrence of Negligence' Reduce the Risk of Catastrophic Terrorism?" (Draft 1.7). Paper prepared for the 2006 Annual Meeting of the American Political Science Association, Philadelphia, PA, August 30–September 3, 2006.

- Broad, William J. "Addressing the Unthinkable, U.S. Revives Study of Fallout." *The New York Times*, March 19, 2004. <http://www.nytimes.com/2004/03/19/us/addressing-the-unthinkable-us-revives-study-of-fallout.html?scp=1&sq=Addressing%20the%20Unthinkable&st=cse&pagewanted=all> (accessed May 25, 2009).
- _____. "New Team Plans to Identify Nuclear Attackers." *The New York Times*, February 2, 2006. <http://query.nytimes.com/gst/fullpage.html?res=9E01E0DA1F3FF931A35751C0A9609C8B63&sec=&spon=&pagewanted=all> (accessed May 17, 2009).
- Bunn, Matthew, and Anthony Wier. "Terrorist Nuclear Weapon Construction: How Difficult?" *Annals of the American Academy of Political and Social Science* 607 (September 2006): 133–149.
- Bunn, Matthew. "A Mathematical Model of the Risk of Nuclear Terrorism." *Annals of the American Academy of Political and Social Science* 607 (September 2006): 103–120.
- _____. *Securing the Bomb 2008*. Cambridge, MA: Project on Managing the Atom, Harvard University and Nuclear Threat Initiative, 2008.
- _____. *The Risk of Nuclear Terrorism—and Next Steps to Reduce the Danger*. Written Testimony before U.S. Senate Committee on Homeland Security and Governmental Affairs, April 2, 2008. <http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=42449878-5e68-4eef-978d-8e671fed2ab0> (accessed May 6, 2009).
- Carter, Ashton B., Michael M. May, and William J. Perry. *The Day After: Action in the 24 Hours Following a Nuclear Blast in an American City*. Cambridge, MA: Preventive Defense Project, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2007. http://belfercenter.ksg.harvard.edu/publication/2140/day_after.html (accessed May 25, 2009).
- Colby, Elbridge A. "Expanded Deterrence: Broadening the Threat of Retaliation." *Policy Review* no. 149 (June/July 2008): 43–59.
- Comprehensive Test Ban Treaty Organization. "Verification Regime: CTBTO Preparatory Commission." <http://www.ctbto.org/verification-regime/> (accessed May 26, 2009).
- Corr, Anders. "Deterrence of Nuclear Terror: A Negligence Doctrine." *The Nonproliferation Review* 12, no. 1 (2005): 127–147.

- Daly, Sara, John Parachini, and William Rosenau. *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism*. Santa Monica, CA: RAND Corporation, 2005.
- Davis, Paul K., and Brian M. Jenkins. *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*. Santa Monica, CA: RAND Corporation, 2002.
- Defense Science Board Task Force. *Nuclear Deterrence Skills*. Washington, DC: Office of the Under Secretary of Defense, 2008.
- Dunlop, William, and Harold Smith. "Who did it? Using International Forensics to Detect and Deter Nuclear Terrorism." *Arms Control Today* 36, no. 8 (October 2006): 6–10.
- Dunn, Lewis A. "Can Al Qaeda Be Deterred From Using Nuclear Weapons?" In *Weapons of Mass Destruction and Terrorism*, edited by Russell D. Howard and James J.F. Forest, 295–316. New York: McGraw-Hill, 2007.
- Federal Bureau of Investigation. "Weapons of Mass Destruction Homepage." http://www.fbi.gov/hq/nsb/wmd/wmd_home.htm (accessed June 5, 2009).
- Ferguson, Charles D. "Can Nuclear Forensics Trace a Detonated Nuclear Weapon to its Source?" Paper prepared for the 2006 Annual Meeting of the American Political Science Association, Philadelphia, PA, August 30–September 3, 2006.
- Ferguson, Charles D., and William C. Potter. *The Four Faces of Nuclear Terrorism*. Monterey, CA: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004.
- Freedman, Lawrence. *Deterrence*. Malden, MA: Polity Press, 2004.
- Frost, Robin. "Nuclear Terrorism after 9/11." *Adelphi Papers* 45, no. 378 (2005): 7–88.
- Gallucci, Robert L. "Averting Nuclear Catastrophe." *Harvard International Review* 26, no. 4 (2005).
- . "Averting Nuclear Catastrophe: Contemplating Extreme Responses to U.S. Vulnerability." *Annals of the American Academy of Political and Social Science* 607 (September 2006): 51–58.
- Garfinkle, Adam. "Does Nuclear Deterrence Apply in the Age of Terrorism?" *Foreign Policy Research Institute Footnotes* 14, no. 10 (May 2009), <http://www.fpri.org/footnotes/1410.200905.garfinkle.nucleardeterrenceterrorism.html> (accessed June 17, 2009).
- George, Alexander L. "The Need for Influence Theory and Actor-Specific Behavioral Models of Adversaries." *Comparative Strategy* 22, no. 5 (2003): 463–487.

- Global Security. "Defense Support Program." <http://www.globalsecurity.org/space/systems/dsp.htm> (accessed May 25, 2009).
- Graham, Bob, Jim Talent, Graham Allison, Robin Cleveland, Steve Rademaker, Tim Roemer, Wendy Sherman, Henry Sokolski, and Rich Verma. *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*. New York, NY: Vintage Books, 2008.
- Harney, Robert C. "Inaccurate Prediction of Nuclear Weapons Effects and Possible Adverse Influences on Nuclear Terrorism Preparedness." *Homeland Security Affairs* 5, no. 3 (September 2009). <http://www.hsaj.org/?article=5.3.3> (accessed October 31, 2009).
- Homeland Security Council. *National Planning Scenarios: Executive Summaries*. (Version 2.0). Washington, DC, 2004.
- Huth, Paul K. "Deterrence and International Conflict: Empirical Findings and Theoretical Debates," *Annual Review of Political Science* 2 (1999): 25–48.
- Institute for Science and International Security. "Global Stocks of Nuclear Explosive Materials: Summary Tables and Charts." ISIS Web site. http://isis-online.org/global_stocks/end2003/summary_global_stocks.pdf (accessed September 12, 2009).
- International Atomic Energy Agency. "Nuclear Forensics Support." *IAEA Nuclear Security Series* 2 (2006).
- International Institute for Strategic Studies. *Nuclear Black Markets: Pakistan, AQ Khan and the Rise of Proliferation Networks*. London: IISS, 2007.
- Jenkins, Brian Michael. *Will Terrorists Go Nuclear?* Amherst, NY: Prometheus Books, 2008.
- Jervis, Robert L. "The Confrontation between Iraq and the U.S.: Implications for the Theory and Practice of Deterrence." *European Journal of International Relations* 9, no. 2 (2003): 315–337.
- Joint Working Group of the American Physical Society and the American Association for the Advancement of Science. *Nuclear Forensics: Role, State of the Art, and Program Needs*. 2008. <http://cstsp.aaas.org/files/Complete.pdf> (accessed May 17, 2009).
- Kapur, S. Paul. "Deterring Nuclear Terrorists." In *Complex Deterrence: Strategy in the Golden Age*, edited by T. V. Paul, Patrick M. Morgan, and James J. Wirtz, 109–130. Chicago: University of Chicago Press, 2009.

- Knopf, Jeffrey W. "Deterrence or Preemption?" *Current History* 105, no. 694 (November 2006): 395–399.
- _____. "The Fourth Wave in Deterrence Research." (unpublished manuscript, Naval Postgraduate School, June 2009).
- _____. "Wrestling with Deterrence: Bush Administration Strategy after 9/11." *Contemporary Security Policy* 29, no. 2 (2008): 229–265.
- Lebovic, James H. *Deterring International Terrorism and Rogue States: U.S. National Security Policy after 9/11*. New York, NY: Routledge, 2007.
- Lebow, Richard Ned. *Between Peace and War: The Nature of International Crisis*. Baltimore: Johns Hopkins University Press, 1981.
- Levi, Michael A. *Deterring State Sponsorship of Nuclear Terrorism*. New York, NY: Council on Foreign Relations, 2008.
- Lieberman, Joseph. *Preventing Nuclear Terrorism: Hard Lessons Learned From Troubled Investments?* Chairman's Opening Statement for the U.S. Senate Committee on Homeland Security and Governmental Affairs, September 25, 2008. <http://hsgac.senate.gov/public/files/092508JILOpen.pdf> (accessed September 22, 2009).
- Lugar, Richard G. "The Nunn-Lugar Cooperative Threat Reduction Program." Official U.S. Senate Web site of Senator Richard G. Lugar. <http://lugar.senate.gov/nunnlugar/> (accessed November 7, 2009).
- Majidi, Vahid. Written Testimony before the U.S. House of Representatives Homeland Security Committee, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, October 10, 2007. <http://homeland.house.gov/SiteDocuments/20071010175326-18735.pdf> (accessed June 16, 2009).
- May, Michael, Jay Davis, and Raymond Jeanloz. "Preparing for the Worst." *Nature* 443, no. 7114 (October 26, 2006): 907–908.
- McCreight, Robert, and Stanley Supinski. "Post-Strike Attribution-A Political & Scientific Dilemma." *Journal of Homeland Security and Emergency Management* 4, no. 2, article 11 (2007). <http://www.bepress.com/jhsem/vol4/iss2/11/> (accessed May 17, 2009).
- Medalia, Jonathan. *Detection of Nuclear Weapons and Materials: Science, Technologies, Observations*. CRS Report R40154. Washington, DC: Congressional Research Service, 2009.

- Miller, Michael. "Nuclear Attribution as Deterrence." *The Nonproliferation Review* 14, no. 1 (2007): 33–60.
- Moody, Kenton J., Ian D. Hutcheon, and Patrick M. Grant. *Nuclear Forensic Analysis*. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2005.
- Mowatt-Larssen, Rolf. *Nuclear Terrorism: Assessing the Threat to the Homeland*. Written Testimony before U.S. Senate Committee on Homeland Security and Governmental Affairs, April 2, 2008.
<http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=42449878-5e68-4eef-978d-8e671fed2ab0> (accessed May 6, 2009).
- Mueller, John. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why we Believe them*. New York, NY: Free Press, 2006.
- Office of the President of the United States of America. *National Strategy for Combating Terrorism*. Washington, DC: Government Printing Office, 2006.
- Parachini, John. "Putting WMD Terrorism into Perspective." *The Washington Quarterly* 26 (Autumn 2003): 37–50.
- Phillips, Matthew. "Uncertain Justice for Nuclear Terror: Deterrence of Anonymous Attacks through Attribution." *Orbis* 51, no. 3 (2007): 429–446.
- Press, Daryl G. *Calculating Credibility: How Leaders Assess Military Threats*. Ithaca, NY: Cornell University Press, 2005.
- Price, Richard, and Nina Tannenwald. "Norms and Deterrence: The Nuclear and Chemical Weapons Taboos." In *The Culture of National Security: Norms and Identity in World Politics*, edited by Peter J. Katzenstein, 114–152. New York: Columbia University Press, 1996.
- Richelson, Jeffrey T. *Defusing Armageddon: Inside NEST, America's Secret Nuclear Bomb Squad*. New York, NY: W. W. Norton & Company, Inc., 2009.
- . *Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea*. New York, NY: W. W. Norton & Company, Inc., 2007.
- Sanger, David E. "Strife in Pakistan Raises U.S. Doubts over Nuclear Arms." *New York Times*, May 4, 2009.
http://www.nytimes.com/2009/05/04/world/asia/04nuke.html?_r=1&scp=1&sq=pakistan nuclear may 4 2009&st=cse (accessed June 13, 2009).
- Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

Schwartz, Stephen I., and Deepti Choubey. *Nuclear Security Spending: Assessing Costs, Examining Priorities*. Washington, DC: Carnegie Endowment for International Peace, 2009.

Smith, David K. "International Nuclear Forensics as Part of a National Program to Safeguard Nuclear Materials." Paper prepared for the American Association for the Advancement of Science 2008 Annual Meeting, Boston, MA, February 16, 2008. <http://cstsp.aaas.org/files/dksmith.pdf> (accessed May 31, 2009).

Snyder, Glenn H. *Deterrence by Denial and Punishment*. Princeton, NJ: Princeton University Center of International Studies, 1959.

Stern, Jessica. *The Ultimate Terrorists*. Cambridge, MA: Harvard University Press, 1999.

Talmadge, Caitlin. "Deterring a Nuclear 9/11." *The Washington Quarterly* 30, no. 2 (2007): 21–34.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*. Washington, DC, 2005.

U.S. Air Force. "Factsheets: WC-135 Constant Phoenix." <http://www.af.mil/information/factsheets/factsheet.asp?fsID=192> (accessed May 30, 2009).

U.S. Congress. "H.R. 730—Nuclear Forensics and Attribution Act." The Library of Congress, THOMAS. <http://thomas.loc.gov/cgi-bin/bdquery/z?d111:HR730>: (accessed May 3, 2009).

U.S. Customs and Border Protection. *Container Security Initiative: 2006–2011 Strategic Plan*. Washington, DC: U.S. Customs and Border Protection, 2006.

_____. *Securing the Global Supply Chain: Customs-Trade Partnership against Terrorism (C-TPAT) Strategic Plan*. Washington, DC: U.S. Customs and Border Protection, 2004.

U.S. Department of Defense, Defense Threat Reduction Agency. "Cooperative Threat Reduction." <http://www.dtra.mil/oe/ctr/index.cfm> (accessed May 3, 2009).

U.S. Department of Energy. "National Nuclear Security Administration—Office of Global Threat Reduction." http://nnsa.energy.gov/nuclear_nonproliferation/1550.htm (accessed May 3, 2009).

_____. National Nuclear Security Administration Website. "Megaports Program Coming to Jamaica." <http://nnsa.energy.gov/news/1039.htm> (accessed September 24, 2009).

- U.S. Department of State. "Proliferation Security Initiative."
<http://www.state.gov/t/isn/c10390.htm> (accessed June 17, 2009).
- U.S. *Fed News Service, Including U.S. State News*. "Rep. Thompson Issues Statement in Support of Nuclear Forensics and Attribution Act." March 25, 2009.
- U.S. House of Representatives, Permanent Select Committee on Intelligence.
Recognizing Iran as a Strategic Threat: An Intelligence Challenge for the United States. Washington, DC: U.S. House of Representatives, 2006.
<http://intelligence.house.gov/media/pdfs/iranreport082206v2.pdf> (accessed June 4, 2009).
- White, Josh. "In Error, B-52 Flew over U.S. with Nuclear-Armed Missiles." *The Washington Post*, September 6, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/05/AR2007090500762.html> (accessed September 24, 2009).
- Zenko, Micah. "Intelligence Estimates of Nuclear Terrorism." *Annals of the American Academy of Political and Social Science* 607 (September 2006): 87–102.

BIBLIOGRAPHY

- Allen, Charles E. *Nuclear Terrorism: Assessing the Threat to the Homeland*. Written Testimony before U.S. Senate Committee on Homeland Security and Governmental Affairs, April 2, 2008.
<http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=42449878-5e68-4eef-978d-8e671fed2ab0> (accessed May 6, 2009).
- Allison, Graham. "Deterring Kim Jong Il." *The Washington Post*, October 27, 2006.
- _____. "Nuclear Accountability." *Technology Review* 108, no. 7 (July 2005): 43.
- _____. "Preface." *Annals of the American Academy of Political and Social Science* 607 (September 2006): 6–9.
- Aloise, Gene. *Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation Radiation Detection Equipment*. United States Government Accountability Office. Written Testimony before U.S. House of Representatives Subcommittee on Investigations and Oversight, Committee on Science and Technology, September 18, 2007. GAO-07-1247T.
- _____. *Combating Nuclear Smuggling: Lessons Learned from DHS Testing of Advanced Radiation Detection Portal Monitors*. United States Government Accountability Office. Written Testimony before U.S. House of Representatives Subcommittee on Investigations and Oversight, Committee on Science and Technology, June 25, 2009. GAO-09-804T. <http://www.gao.gov/new.items/d09804t.pdf> (accessed September 24, 2009).
- Bakier, Abdul Hameed. "Jihadis Discuss Plans to Seize Pakistan's Nuclear Arsenal." *Terrorism Monitor* 7, no. 14 (May 26, 2009): 4–5.
http://www.jamestown.org/uploads/media/TM_007_19.pdf (accessed June 2, 2009).
- Benjamin, Daniel, and Steven Simon. "The Next Debate: Al Qaeda Link." *The New York Times*, July 20, 2003.
<http://www.nytimes.com/2003/07/20/opinion/20BENJ.html?scp=2&sq=The%20Next%20Debate:%20Al%20Qaeda%20Link&st=cse> (accessed May 17, 2009).
- Biden, Joe. "CSI: Nukes." *Wall Street Journal*, June 4, 2007.
- Biesecker, Calvin. "DHS Establishes Center for Nuclear Forensics." *Defense Daily* 231, no. 76 (October 23, 2006): 1.
- Bleek, Phillip C. "Preparing for the day after: Post nuclear-terrorism attribution, cooperation, transparency, obfuscation" (Draft 1.3.) Paper prepared for the 2007 International Studies Association Conference, Chicago, IL, February 20, 2007.

- Bunn, Matthew. *Preventing Nuclear Terrorism: An Agenda for the Next President*. Cambridge, MA: Project on Managing the Atom, Harvard University and Nuclear Threat Initiative, 2008.
- Byman, Daniel. *Iran, Terrorism, and Weapons of Mass Destruction*. Prepared Remarks for the Hearing entitled “WMD Terrorism and Proliferant States” before the Homeland Security Committee, Subcommittee on Prevention of Nuclear and Biological Attack, September 8, 2005.
<http://www.brookings.edu/views/testimony/fellows/byman20050908.pdf> (accessed June 4, 2009).
- Cameron, Gavin. “Nuclear Terrorism Reconsidered.” *Current History* 99, no. 636 (April 2000): 154–157.
- Carter, Ashton B. “How to Counter WMD.” *Foreign Affairs* 83, no. 5 (2004): 72–85.
- Castillo, Jasen J. “Nuclear Terrorism: Why Deterrence Still Matters.” *Current History* 102, no. 668 (December 2003): 426–431.
- Chivers, Daniel H., Bethany F. Lyles Goldblum, Brett H. Isselhardt, and Jonathan S. Snider. “Attribution and Information Sharing in Nuclear Forensics.” *Arms Control Today* 38, no. 6 (July/August 2008): 24.
- _____. “Before the Day After: Using Pre-Detonation Nuclear Forensics to Improve Fissile Material Security.” *Arms Control Today* 38, no. 6 (July/August 2008): 22–27.
- Colby, Elbridge A. “The New Deterrence: Overwhelming and Searching Retaliation.” *The Weekly Standard*, April 10, 2008.
<http://www.weeklystandard.com/content/public/articles/000/000/014/959tnykn.asp?pg=1> (accessed September 12, 2009).
- Davis, Jay. “After A Nuclear 9/11.” *The Washington Post*, March 25, 2008.
- _____. “The Attribution of WMD Events.” *Journal of Homeland Security* (April 2003).
<http://www.homelandsecurity.org/journal/Search.aspx?s=The+Attribution+of+WMD+Events> (accessed May 17, 2009).
- Dershowitz, Alan M. *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*. New Haven, CT: Yale University Press, 2002.
- Doll, Abby. “Anti-Nuclear Terrorism Strategies Discussed.” *Arms Control Today* 37, no. 6 (July/August 2007): 33–34.
- Dunlop, William, and Harold Smith. “Post-Detonation Nuclear Forensics.” *Arms Control Today* 36, no. 8 (October 2006): 9.

- Gallaway, Charles R. *Opening Statement*. Written Testimony before the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, June 9, 2009.
<http://homeland.house.gov/SiteDocuments/20090609142104-36264.pdf> (accessed June 15, 2009).
- Grotto, Andrew, and Joe Cirincione. *Orienting the 2009 Nuclear Posture Review: A Roadmap*. Washington, DC: Center for American Progress, 2008.
- Hecker, Siegfried S. "Toward a Comprehensive Safeguards System: Keeping Fissile Materials out of Terrorists' Hands." *Annals of the American Academy of Political and Social Science* 607 (September 2006): 121–132.
- Helfstein, Scott, Michael J. Meese, Don Ressler, Reid Sawyer, Troy Schnack, Mathew Shieffer, Scott Silverstone, and Scott Taylor. *Terrorism, Deterrence and Nuclear Weapons*. White Paper Prepared for the Secretary of Defense Task Force on DoD Nuclear Weapons Management. West Point, NY: Combating Terrorism Center, U.S. Military Academy, 2008.
<http://se1.isn.ch/serviceengine/FileContent?serviceID=47&fileid=109F8732-DEDD-39D2-FF58-F90DB28C8DC7&lng=en> (accessed July 16, 2009).
- Hirsch, Theodore. "The IAEA Additional Protocol: What it is and why it Matters." *The Nonproliferation Review* 11, no. 3 (2004).
- James Martin Center for Nonproliferation Studies, Monterey Institute of International Studies. "NTI: Databases: UN Resolution 1540." Nuclear Threat Initiative Web site.
<http://www.nti.org/db/1540/index.html> (accessed April 26, 2009).
- Kamp, Karl-Heinz. "An Overrated Nightmare." *Bulletin of the Atomic Scientists* 52, no. 4 (July/August 1996): 30–34.
- Kokoshin, Andrei. "A Nuclear Response to Nuclear Terror: Reflections of Nuclear Preemption." *Annals of the American Academy of Political and Social Science* 607 (September 2006): 59–63.
- Levi, Michael A. "Deterring Nuclear Terrorism." *Issues in Science and Technology* 20, no. 3 (Spring 2004): 70–73.
- _____. *On Nuclear Terrorism*. Cambridge, MA: Harvard University Press, 2007.
- Lobsenz, George. "NNSA: New Projects Needed for More than Weapons." *Defense Daily* 241, no. 49 (March 18, 2009).
- Montgomery, Evan Braden. *Nuclear Terrorism: Assessing the Threat, Developing a Response*. Washington, DC: Center for Strategic and Budgetary Assessments, 2009.
http://www.csbaonline.org/4Publications/PubLibrary/R.20090422.Nuclear_Terrorism/R.20090422.Nuclear_Terrorism.pdf (accessed July 16, 2009).

- Mowatt-Larssen, Rolf. "Preventing Nuclear Terrorism: A Global Intelligence Imperative." The Washington Institute for Near East Policy. <http://www.washingtoninstitute.org/templateC05.php?CID=3048> (accessed May 3, 2009).
- Mueller, John. "False Alarms." *The Washington Post*, September 29, 2002. <http://proquest.umi.com/pqdweb?did=198466581&Fmt=7&clientId=11969&RQT=309&VName=PQD> (accessed June 10, 2009).
- _____. "Harbinger or Aberration? A 9/11 Provocation." *The National Interest*, no. 69 (Fall 2002): 45–50.
- National Intelligence Council. *National Intelligence Estimate: The Terrorist Threat to the U.S. Homeland*. Washington, DC: NIC, 2007.
- Niemeyer, Sidney, and David K. Smith. "Following the Clues: The Role of Forensics in Preventing Nuclear Terrorism." *Arms Control Today* 37, no. 6 (July/August 2007): 14–15.
- Nuclear Threat Initiative. "Homeland Security Backs off Funding for Nuclear-Detection Technology." *Global Security Newswire*, May 8, 2009. http://www.globalsecuritynewswire.org/gsn/nw_20090508_6590.php (accessed August 30, 2009).
- OxResearch. "INTERNATIONAL: Extended Deterrence Needs Cooperation." (January 25, 2007).
- _____. "U.S./INTERNATIONAL: Nuclear Counter-Terror Effort Evolves." (June 5, 2007).
- Panel on Understanding Terrorists in Order to Deter Terrorism. *Discouraging Terrorism: Some Implications of 9/11*. Washington, DC: The National Academies Press, 2002.
- Perkovich, George, Joseph Cirincione, Rose Gottemoeller, Jon B. Wolfsthal, and Jessica T. Mathews. *Universal Compliance: A Strategy for Nuclear Security*. Washington, DC: Carnegie Endowment for International Peace, 2004.
- Saradzhyan, Simon. "Russia: Grasping the Reality of Nuclear Terror." *Annals of the American Academy of Political and Social Science* 607 (September 2006): 64–77.
- Sciolino, Elaine, William J. Broad, and David E. Sanger. "Iran's Secrecy Widens Gap in Nuclear Intelligence." *New York Times*, May 19, 2006.
- Tannenwald, Nina. "Stigmatizing the Bomb: Origins of the Nuclear Taboo." *International Security* 29, no. 4 (Spring 2005): 5–49.

- U.S. Customs and Border Protection. CBP.gov Web site. “Customs-Trade Partnership Against Terrorism: A Year in Review.”
http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2008_news_releases/jan_2008/01312008.xml (accessed September 24, 2009).
- U.S. Department of Homeland Security. “Office of Grants and Training-Exercises.”
<http://www.ojp.usdoj.gov/odp/exercises.htm> (accessed June 5, 2009).
- U.S. Fed News Service, Including U.S. State News*. “Rep. Schiff Introduces Nuclear Forensics and Attribution Act.” February 9, 2009.
- . “Washington State University Scientists Awarded Over \$2 Million to Study Nuclear Forensics, Radiation Detectors.” October 10, 2008.
- U.S. Government Accountability Office. *Combating Nuclear Smuggling: DHS Improved Testing of Advanced Radiation Detection Portal Monitors, but Preliminary Results Show Limits of the New Technology*. GAO-09-665. Washington, DC: U.S. GAO, 2009.
- U.S. Nuclear Regulatory Commission. “NRC: Special Nuclear Materials.”
<http://www.nrc.gov/materials/sp-nucmaterials.html> (accessed June 12, 2009).
- Whiteneck, Daniel. “Deterring Terrorists: Thoughts on a Framework.” *Washington Quarterly* 28, no. 3 (2005): 187–199.
- Wilson, Elizabeth K. “Handling Nuclear Evidence.” *Chemical & Engineering News* 83, no. 41 (2005): 40.
- Wisconsin Project on Nuclear Arms Control. “Iran Watch Bulletin: Illicit Chinese Exports to Iran—4-8-09.” <http://www.iranwatch.org/ourpubs/bulletin/chinese-exports-iran-040809.htm> (accessed April 25, 2009).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. U.S. Department of Homeland Security
Domestic Nuclear Detection Office
Washington, DC